E-MAIL IN THE WORKPLACE: USE AT YOUR OWN RISK

*Carol E. Bast**

Most of us have become so accustomed to the convenience of e-mail and the speed with which it allows us to communicate that we could not imagine a work day without it. At times you may have used an e-mail message to vent some steam over a problem at work. Before you do so in an e-mail message you should consider how comfortable you would be if your employer accessed the message. An injudicious e-mail may put your job at risk.

For example, on November 30, 1999 the New York Times Co. fired twenty- two employees in Norfolk, Virginia and one employee in New York City for sending offending e-mails. Approximately twenty more employees who had received offending e-mails, but who had not sent offending e-mails, received warning letters. The offending e-mails violated the New York Times company e-mail policy. "[Cjomputer communications must be consistent with conventional standards of ethical and proper conduct, behavior and maimers and are not to be used to create, forward or display any offensive or disruptive messages, including photographs, graphics and audio material."[1]

No one, not even a federal judge, is safe from monitoring. In December of 2000, the Administrative Office of the United States Courts began to monitor the Internet usage of federal judges and their staffs. The office sent letters to chief judges informing them of computers that had accessed questionable Internet sites. In May of 2001, a committee of judges from the federal Court of Appeals for the Ninth Circuit voted to disable the monitoring software.[2] At its September 2001 meeting the United State Judicial Conference adopted a modified resolution that allows limited monitoring of the web sites accessed but allows no monitoring of e-mail.[3]

Judge Kozinski, a judge on the Court of Appeals for the Ninth Circuit, had been one of the most severe critics of the proposed monitoring policy being considered by the United States Judicial Conference. In an editorial appearing in the *Wall Street Journal*, Judge Kozinski railed against the proposed policy. "At the heart of the policy is a warning—very much like that given to federal prisoners—that every employee must surrender privacy as a condition of using common office equipment. The judge imagined the types of communication that might be subject to scrutiny by some bureaucrat. "Judicial opinions, memoranda to colleagues, phone calls to your

* Associate Professor, Department of Criminal Justice and Legal Studies, University of Central Florida; Member, Florida Bar; J.D., 1982, New York Law School; M.A., 1976, University of Wisconsin-Madison; B.A., 1974, Kalamazoo College.

[1] Ann Carms, *Prying Times: Those Bawdy E-Mails Were Good for a Laugh; Until the Ax Fell; The Close- Knit Staff Shared Jokes, but Didn 't Realize Bosses Were Watching; A Special 'Funnies' Folder,* WALL St. J., Feb. 4,2000, at Al.

[2] Maura Dolan, *The State Defiant Judges Bar Monitoring of Staff Net Use Internet: Software was disabled after 9th Circuit jurists approved the move. Panel headed by Chief Justice Rehnquist will decide whether to restore it,* L.A. TIMES, Aug. 9,2001, at B10.

[3] Philip L. Gordon, *Federal Judges * Victory Just the First Shot in the Battle Over Workplace Monitoring* (Sept. 20, 2001), at http://www.privacyfoundation.org/workplace/law/law_show.asp7id 75&action 0.

proctologist, faxes to your bank, e-mails to your law clerks, prescriptions you fill online - you must agree that bureaucrats are entitled to monitor and record them all."[4]

This paper examines the legal status of e-mail messages. The following sections review employer monitoring of employee e-mail messages, the protection afforded them under the federal statutes, and cases concerning interception and retrieval of e-mail messages. The paper then suggests amendments to the federal statutes.

I. EMPLOYER MONITORING

Employer monitoring of e-mail messages is more prevalent that one might think. The American Management Association survey of major United States firms revealed that forty-five percent of these firms monitor their employees' e-mails.[5] In addition, the percentage of employers monitoring employees' e-mails appears to be steadily on the rise. The recent figure is eighteen percentage points above what it was two years before. The American Management Association's 1999 survey revealed that twenty seven percent of the employers surveyed monitored employee e- mails.[6] In addition, many employers monitor employees' online activities. The American Management Association conducted a survey in July of 2001 of 435 large United States companies. The survey revealed that over sixty percent of those companies monitored employee Internet connections.[7]

The Privacy Foundation conducted a study that showed employer monitoring of employee Internet and e-mail is pervasive. The study found that fourteen million United States employees have their Internet or e-mail use monitored by employers.[8] The Privacy Foundation, a Denver nonprofit organization, hosts a web site[9] that maintains information concerning surveillance. Additionally, a portion of this web site entitled "Workplace Surveillance Project" collects "articles, interviews, and resources [concerning] workplace surveillance." Privacy advisories accessible at the site are rated from one to five windows, with the five-window rating being the most intrusive.[10]

Why do employers monitor employee e-mail? One reason often given is to curb time spent by employees on personal business. One manufacturer of a software monitoring program estimates that employee productivity lost as a result of employees pursuing personal business while on company time totals $63 billion annually.[11] Another prime reason for employer monitoring is the fear that the employer may be

[4] Alex Kozinski, *Privacy on Trial*, Wall St. J., Sept. 4,2001, at A22.

[5] Michael Starr & Jordan Lippner, *Monitoring Employee E-mail,* NAT'L L.J., June 11,2001, at B8.

[6] Wendy R, Leibowitz, *E-Litigation: E-mail Law Expands,* Nat'L L.J., July 19,1999, at B8.

[7] Ted Bridis & Glenn R. Simpson, *Judges' Ire Stirs Debate on Web Monitoring,* WALL ST. J., Aug. 9, 2001, at B9.

[8] Carrie Kirby, *The boss may be spying/Net use easy to monitor,* S.F. CHRON., July 9,2001, at D.l.

[9] http://www.privacyfoundation.org

[10] *Privacy Watch,* http://www.privacyfoundation.org/privacywatch/index.asp (last visited May 16,2003).

[11] Kirby, *supra* note 8.

held vicariously liable for sexually explicit or otherwise offensive e-mails sent by employees. That type of e-mail has the potential for supporting claims of a hostile workplace environment, sexual harassment, or discrimination based on sex, age, race, or religion.[12] In addition, certain industries, such as the securities industry, are regulated with respect to information that may be communicated outside the firm. Compliance with Securities and Exchange Commission rules or other regulations may necessitate employer monitoring of employee e-mail.[13] Other employer concerns include loss of trade secrets or other employer proprietary information as well as employer liability for copyright infringement. Trade secrets and other proprietary information can be at risk through misdirected e-mail messages or unauthorized entry by a third party to the employer's computer network. As far as copyright is concerned, an employee may acquire copyrighted software and use it without proper authorization. Employee use of such software may subject the employer to liability.[14]

The Internet is comprised of a vast network of computers. When someone sends an e-mail message, the message does not travel as a single document. The message is broken up into segments called "packets." The packets travel separately by a variety of routes, with the packets combined into a single e-mail message when the packets reach their destination. Each packet travels from the sender's computer through numerous other computers before arriving at its destination. Each computer through which a packet travels makes a temporary or intermediate copy of the packet until the packet safely arrives at the next computer in the chain. This "store and forward" method requires that each computer retain this temporary or intermediate copy of the packet until the next computer in the chain confirms that the packet has successfully arrived.[15] Because each e-mail message is divided into packets that travel separately during transmission, it is difficult to intercept an e-mail message during transmission. "Eavesdroppers must know exactly what they are looking for and when it will be transmitted, and be fortunate enough to both guess the path that the messages will take and discover packets with significant information. [Therefore,] there [is] 'virtually no risk' of such interception."[16] Eavesdropping on an e- mail message during its transmission requires an eavesdropper with knowledge of the technology. "[W]hile any thief can break into a file cabinet or office, 'sniffing out' sensitive e-mails requires an uncommon degree of sophistication."

The following section examines how e-mail messages are protected under the federal statutes.

[12] Allison R. Michael & Scott M. Lidman, *Monitoring of Employees Still Growing: Employers Seek Greater Productivity and Avoidance of Harassment Liability; Most Workers Have Lost on Privacy Claims,* NAT'L L.J., Jan. 29,2001, at B9.

[13] Kirby, *supra* note 8.

[14] Amy Rogers, *You Got Mail but Your Employer Does Too: Electronic Communication and Privacy in the 21st Century Workplace,* 5 J. TECH. L. & POL'Y 1, 6, 7 (2000).

[15] Brian D. Wassom, *A Reasonable Expectation of Privacy: Can Michigan Attorneys Safely Use Unencrypted Internet E-Mail for Confidential Communications?,* 78 MICH. B. J. 590, 590 (1999).

[16] *Id.*

17 Id.

II. FEDERAL STATUTES

Chapters 119 and 121 of Title 18 of the United States Code protect certain types of communications. Chapter 119 encompasses sections 2510 through 2522 of Title 18[18] and chapter 121 encompasses sections 2701 through 2711 of Title 18.[19] Chapter 119 is sometimes hereinafter referred to as the "Federal Wiretap Act." Chapter 121 is sometimes hereinafter referred to as the "Stored Communications Act." The three protected types of communication are "oral communication," "wire communication," and "electronic communication." Basically, oral communication is a face-to-face conversation.[20] Wire communication is a telephone conversation audible by the human ear at some point.[21] Electronic communication[22] is a digitally transmitted message. Neither wire communication nor electronic communication includes the electronic storage of the communication.

These federal statutes, when adopted in 1968, were designed to legally protect oral communication and wire communication against interception.[23] Advances in technology required Congress to amend the statutes in 1986 to add a new

[18] 18 U.S.C.S. §§ 2510 - 2522 (LEXIS 1993 & Supp. 2002).

[19] 18 U.S.C.S. §§ 2701 - 2711 (LEXIS 1993 & Supp. 2002).

[20] The Federal Wiretap Act defines "oral communication" as "any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication." 18 U.S.C.S. § 2510(2) (LEXIS 1993).

[21] The Federal Wiretap Act defines "wire communication" as

> any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce;

18 U.S.C.S. § 2510(1) (LEXIS 1993 & Supp. 2002).

[22] The Federal Wiretap Act defines "electronic communication" 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, photo- electronic 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;
> (C) any communication from a tracking device (as defined in section 3117 of this title); or
> (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds.

18 U.S.C.S. § 2510(12) (LEXIS 1993 & Supp. 2002).

[23] OMNIBUS CRIME CONTROL AND SAFE STREETS ACT OF 1968, Pub. L. 90-351, § 801 (b), 82 Stat. 197 (1968), *reprinted in* 1968 U.S.C.C.A.N. 237,253.

category of protected communication, that of electronic communication.[24] This new category of electronic communication" was intended to include electronic mail.[25] The glossary to the Senate Report defined electronic mail as follows:[26]

> Electronic mail is a form of communication by which private correspondence is transmitted over public and private telephone lines. In its most common form, messages are typed into a computer terminal, and then transmitted over telephone lines to a recipient computer operated by an electronic mail company. If the intended addressee subscribes to the service, the message is stored by the company's computer "mail box" until the subscriber calls the company to retrieve its mail, which is then routed over the telephone system to the recipient's computer....
>
> Electronic mail systems may be available for public use or may be proprietary, such as systems operated by private companies for internal correspondence.

Chapter 119 of Title 18 of the United States Code, entitled "Wire and Electronic Communications Interception and Interception of Oral Communications," prohibits the interception of oral, wire, and electronic communication.[27] This chapter criminalizes the interception of such communications as well as the use or disclosure of illegally intercepted communications.[28] It also provides for civil damages to one whose communication has been illegally intercepted. Further, awards may include reasonable attorney's fees and litigation costs.[29] Illegally intercepted oral and wire communications are inadmissible at trial. However, no exclusionary relief is available to one whose electronic communication has been illegally intercepted.[30]

Chapter 119 allows the interception of oral, wire, and electronic communications by law enforcement officers if authorized by court order. The persons allowed to authorize the application are limited, with the persons allowed to authorize the application to intercept an oral or wire communication more limited than the persons allowed to authorize the application to intercept an electronic communication.[31] Authorization may be given to intercept oral and wire communications if the

[24] Senate Report No. 99-541, at 1 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3555.

[25] Senate Report No. 99-541, at 14 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555,3568.

[26] Senate Report No. 99-541, at 8 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555,3562.

[27] The Federal Wiretap Act defines "intercept" as " the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device. 18 U.S.C.S. § 2510(4) (LEXIS 1993).

[28] 18 U.S.C.S. § 2511 (LEXIS 1993 & Supp. 2002).

[29] 18 U.S.C.S. § 2520 (LEXIS 1993 & Supp. 2002).

[30] 18 U.S.C.S. § 2515 (LEXIS 1993).

[31] 18 U.S.C.S. § 2516 (LEXIS 1993 & Supp. 2002). Subsection (1) concerns the procedure to obtain a court order with respect to oral and wire communications. Subsection (3) concerns the procedure to obtain

law enforcement officers are gathering evidence of certain specific crimes. An electronic intercept authorization may be given only if the law enforcement officers are gathering evidence of a federal felony.[32] The procedure for obtaining the court order is detailed in the statute and failure to comply with the statutory procedure may result in the exclusion of any evidence obtained.[33]

The 1986 amendments also added chapter 121 to title 18 of the United States Code. Chapter 121, entitled "Stored Wire and Electronic Communications and Transactional Records Access," prohibits access to wire and electronic communication while in storage.[34] This chapter criminalizes the accessing of stored wire and electronic communications.[35] The chapter provides civil damages to one whose stored wire or electronic communication has been intercepted or whose stored communication has been divulged by the service provider.[36] No exclusionary relief is available to one whose stored wire or electronic communication has been illegally intercepted. A separate statute emphasizes that there is no exclusionary relief for accessing stored communications.[37]

Chapter 121 allows the interception of a stored wire or electronic communication by law enforcement officers if authorized by a warrant.[38] The procedure for obtaining a warrant is much less detailed and easier to follow than the procedure for obtaining a court order under chapter 119. Because compliance with the procedure for obtaining a warrant is easier, there is less likelihood that evidence obtained would be excluded for failure to follow proper procedure.

Both chapters 119 and 121 criminalize certain activities and provide civil damages. The basic criminal penalty for illegal interception or disclosure of illegally intercepted communication is a fine or prison term of up to five years, or both.[39] In other words, illegal interception or disclosure of illegally intercepted communication is a felony. The criminal penalty for the first offense of accessing stored communication is a fine and a maximum prison term of one year. For any additional offense,

a court order with respect to electronic communication. Subsection (2) concerns the procedure necessary for a state authority to obtain a court order with respect to oral, wire, and electronic communications.

[32] *Id.*

[33] 18 U.S.C.S. § 2518 (LEXIS 1993 & Supp. 2002).

[34] The final statute within the Stored Communications Act, 18 U.S.C.S. § 2711 (LEXIS 1993 & Supp. 2002), makes the definitions from the Federal Wiretap Act applicable to the Stored Communications Act. That statute provides: "As used in this chapter--

(1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section." Under 18 U.S.C.S. § 2510(17) (LEXIS 1993 & Supp. 2002), "'electronic storage' means— (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."

[35] 18 U.S.C.S. § 2701 (LEXIS 1993).

[36] 18 U.S.C.S. §§ 2701,2702,2707 (LEXIS 1993 & Supp. 2002).

[37] The statute entitled "Exclusivity of remedies" provides: "The remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter." 18 U.S.C.S. § 2708 (LEXIS 1993).

[38] 18 U.S.C.A. § 2703 (LEXIS 1993 & Supp. 2002).

[39] 18 U.S.C.S. § 2511(4) (LEXIS 1993 & Supp. 2002).

the criminal penalty is a fine and a maximum prison term of five years.[40] There is a criminal penalty for accessing stored communication but not for divulging a stored communication illegally accessed.

Chapters 119 and 121 also include exceptions allowing an e-mail service provider to monitor e-mail messages. Under chapter 119, it is lawful for

> [A]n officer, employee, or agent of a provider of . . . electronic communication service, whose facilities are used in the transmission of [an] electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service.[41]

Thus, a service provider employee may lawfully intercept an electronic communication only if "in the normal course of his employment" and "while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service." Under chapter 121, the exception is much broader. The criminal and civil remedies do not apply to "the person or entity providing a wire or electronic communications service."[42]

The following section discusses cases interpreting chapters 119 and 121 with regard to e-mail messages.

III. CASES CONCERNING INTERCEPTION AND RETRIEVAL OF E-MAIL MESSAGES

One of the main issues considered in cases involving e-mail has been whether the e-mail was intercepted or whether it was accessed as a stored electronic communication. The distinction is usually crucial in determining liability. The e- mail service provider is much more likely to escape criminal and civil liability if the e-mail is determined to have been a stored electronic communication. This is so because the exception for lawful acts of a service provider is much broader for accessing a stored electronic communication than for intercepting an electronic communication.[43]

Steve Jackson Games, Incorporated v. *United States Secret Service* and *Bohach* v. *City of Reno*[44][45] were the first cases to consider the meaning of "intercept" of e-mail and "access" to stored e-mail.

In *Steve Jackson Games,* the Company used one of its computers to operate an electronic bulletin board. The bulletin board was also used as the service provider

[40] 18 U.S.C.S. § 2701(b) (LEXIS 1993 & Supp. 2002).
[41] 18 U.S.C.S. § 2511 (2)(a)(i) (LEXIS Supp. 2002).
[42] 18 U.S.C.S. § 2701(c)(1) (LEXIS 1993).
43. See supra notes 40-41 and accompanying text.
[44] 36 F.3d 457 (5th Cir. 1994).
[45] 932 F. Supp. 1232 (D. Nev. 1996).

for an e-mail service. The computer stored e-mail messages in temporary storage until the addressee read the message. The addressee would either delete the message or store it on the computer hard drive.[46] The United States Secret Service was investigating an individual who apparently had gained unauthorized access to information on a telephone company's emergency call system. The Secret Service obtained a warrant to seize items from Steve Jackson Games. The computer operating the electronic bulletin board was one of the items seized. When the Secret Service seized the computer, it contained 162 unread e-mail messages.[47]

Steve Jackson Games and various individuals sued, claiming that when the Secret Service agents read and deleted the e-mails, they violated the Federal Wiretap Act and the Stored Communications Act. At trial, the federal district court held that the Secret Service had violated the Stored Communications Act and awarded the plaintiffs statutory damages, attorneys' fees, and costs. However, the court held that the Secret Service had not violated the Federal Wiretap Act because it had not intercepted the e-mail messages while in transmission.[48]

The appellate court agreed that the Secret Service had violated the federal Stored Communications Act but not the Federal Wiretap Act, stating that Congress did not intend that the same conduct violate both the Federal Wiretap Act and the federal Stored Communications Act. The court reasoned that the much stricter requirements for obtaining court authorization and conducting an intercept of an electronic communication than for accessing stored electronic communications showed that more protection was afforded to individuals whose e-mail might be intercepted in transmission than individuals whose stored e-mail might be accessed.[49] The reason for this distinction was that someone intercepting e-mail during transmission might unavoidably intercept messages other than the ones targeted. The danger of accessing irrelevant e-mail messages from storage is less because a key word search can be used on stored e-mail messages to retrieve only those targeted.[50]

In *Bohach*, the Reno police department used the "Alphapage" software to transmit short messages to display pagers. Similar to an e-mail message, the sender types the pager message into a computer and then presses the send key. The message goes to the server file, from there it is sent by modem to the paging company, and the paging company sends the message to the receiver pager by radio broadcast.[51] In 1996, two police officers sent each other messages and sent messages to another officer over the Alphapage system. After the Reno police department investigated the content of the messages the two officers sued, claiming that the storage of the messages on the department computer and retrieval of the messages from storage violated the Federal Wiretap Act.[52]

[46] 36 F.3d at 458.
[47] *Id.* at 458,459.
[48] *Id.* at 459,460.
[49] *Id.* at 459,462,463.
[50] *Id.* at 459,463.
[51] 932 F. Supp. at 1234.
[52] «.at 1233.

The court found that the messages were in electronic storage on the police department computer and the city, as the service provider, could lawfully access the messages under 18 U.S.C. § 2701 (c)(1).[53]

Many of the e-mail interception cases involve an employer, who is also the service provider, intercepting an employee's e-mail messages. Typically, the employer takes some type of adverse action with respect to the employee's e-mail messages and the employee alleges that the employer's interception of his or her e- mail messages was illegal. In the first of the following two cases, the employee was discharged based on the employee e-mails that the employer had retrieved. In the second case, the employee was suspended.

In *Smyth* v. *Pillsbury Company*,[54] Pillsbury operated an e-mail system for the use of employees. According to Smyth, Pillsbury had assured its employees that e-mails "would remain confidential and privileged" and that "e-mail communications could not be intercepted and used by [Pillsbury] against its employees as grounds for termination or reprimand."[55] In October 1994, Smyth and his supervisor exchanged some e-mails. In the exchange, Smyth wrote about sales management and threatened, "to kill the backstabbing bastards." He also called a planned holiday party the "Jim Jones Koolaid affair."[56] Later Pillsbury retrieved some of the e-mail messages and informed Smyth on January 17, 1995 that Pillsbury was discharging Smyth, effective February 1, 1995, because the e-mails contained "inappropriate and unprofessional comments."[57]

Smyth filed suit against Pillsbury claiming wrongful discharge. The court granted Pillsbury's motion to dismiss because Smyth had not stated a claim for which the court could grant relief.[58] In its reasoning, the court examined Smyth's claim to determine if there was an invasion of Smyth's privacy such that his discharge would violate public policy. The court found that Smyth had no reasonable expectation of privacy in the e-mails sent to his supervisor because they were "voluntarily made by [Smyth] to his supervisor over the company e-mail system even though Pillsbury had made "assurances that such communications would not be intercepted by management."[59] In addition, the court found that even if Smyth had a reasonable expectation of privacy in his e-mails, Pillsbury'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.

In *McLaren* v. *Microsoft Corporation*, the court followed *Smyth* and rejected McLaren's claim that Microsoft had invaded his privacy when it retrieved

[53] *Id.* at 1237.
[54] 914 F. Supp. 97,98 (E.D. Pa. 1996).
[55] ***Id.***
[56] *Id.* at98&n.l.
[57] *Id.* at 98-99.
[58] *Id.* at 98.
[59] /rf. at 100,101.
[60] *Id.* at 101.
[61] No. 05-97-00824-CV, 1999 WL 339015, at 1 (Tex. App. May 28,1999).

some of McLaren's e-mails. Microsoft had provided McLaren with a computer that he could use to access e-mails from a Microsoft e-mail system. McLaren could move his e-mails from his in-box located on the Microsoft server to password- protected personal folders on his computer.[62] In December of 1996, Microsoft suspended McLaren "pending an investigation into accusations of sexual harassment and 'inventory questions.'"[63] During McLaren's suspension, Microsoft retrieved some of his e-mails personal password-protected folders.[64] Microsoft fired McLaren on December 11, 1996.[65]

The court pointed out that McLaren's e-mails had been transmitted over the Microsoft network and were accessible to Microsoft. The court found that McLaren did not have a reasonable expectation of privacy in his e-mails even though he had moved them into password-protected personal folders.[66] As the *Smyth* court had, the *McLaren* court balanced McLaren's alleged right to privacy against Microsoft's interest in investigating alleged improprieties. The *McLaren* court found that even if McLaren had a reasonable expectation of privacy, it was outweighed by Microsoft's "interest in preventing inappropriate and unprofessional comments, or even illegal activity, over its e-mail system."[67]

Until the Court of Appeals for the Ninth Circuit decided *Konop* v. *Hawaiian Airlines*, /nc.,[68] courts had uniformly held that the penalties for intercepting an electronic communication applied only during the brief time during which an electronic communication was being transmitted. In *Konop*, the plaintiff, an airline pilot, had a website containing information largely critical of the airline. To view the site, one needed a password from Konop and had to agree not to divulge information from the website. The airline vice president obtained the use of another pilot's name and password to access the website. Later the vice president used another pilot's name to access the website.[69]

Konop sued, claiming the airline vice president's access of the website violated the Federal Wiretap Act and Stored Communications Act.[70] On January 8,
2001, the federal Court of Appeals for the Ninth Circuit held that "the [Federal] Wiretap Act protects electronic communications from interception when stored [at a secure website] to the same extent as when in transit."[71] That decision was short lived. The court that had announced the January 8, 2001 decision withdrew it on

[62] *Id.* at *4.

[63] *Id.* at *1.

64 Id. at *1,5.

[65] *Id.* at *1.

66 *Id.* at »4.

[67] *Id.* at *5.

[68] 236 F.3d 1035 (9th Cir. 2001), *opinion withdrawn*, 262 F.3d 972 (9th Cir. 2001), *opinion superceded*, 302 F.3d 868 (9th Cir. 2002).

[69] *Id.* at 1040,1041.

[70] *Id.* at 1041.

71 Id. At 1046, 1048.

August 28, 2001 and issued a new opinion on August 23, 2002, which superceded the first decision.[72]

In the following case, the independent contractor sued the employer because the employer retrieved some of the independent contractor's e-mails.

In *Fraser* v. *Nationwide Mutual Insurance Co.*,[13] Fraser was an insurance agent for Nationwide but was an independent contractor rather than a Nationwide employee. In January of 1990, Fraser leased computer hardware and software from Nationwide. The software included e-mail service maintained by Nationwide.[74] In June of 1996, Fraser and other Nationwide agents formed a Pennsylvania chapter of the Nationwide Insurance Independent Contractors Association. The association's purpose was to protect the role of the independent contractor insurance agents and at times opposed actions taken by Nationwide.[75]

In August of 1998, Nationwide was investigating whether Fraser had sent a letter to Nationwide competitors containing "inappropriate communications." To make this determination, Nationwide searched Fraser's e-mails. Nationwide found that an e-mail sent by Fraser to another Nationwide agent confirmed that the letter had been sent to a Nationwide competitor. The agent had received Fraser's e-mail and discarded it.[76] Nationwide cancelled Fraser's agent's agreement on September 2, 1998.[77]

Fraser sued Nationwide. Among the counts in the complaint, Fraser alleged that Nationwide had intercepted Fraser's e-mail in violation of the federal and Pennsylvania wiretap statutes and that Nationwide had accessed Fraser's e-mail from storage in violation of federal and state statutes concerning stored communications.[78] The court first considered the meaning of the terms "interception" and "access" under the federal and state statutes.[79] The court determined that interception occurs during the transmission of the e-mail message from the sender to the recipient. "Thus, interception of a communication occurs when transmission is interrupted, or in other words when the message is acquired after it has been sent by the sender, but before it is received by the recipient."[80] The court found that "electronic storage" includes the temporary storage of an e-mail message as it is being transmitted but that access to a stored communication does not include "retrieval of a message from

[72] Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002). "We therefore hold that for a website such as IConop's to be 'intercepted' in violation of the Wiretap Act, it must be acquired during transmission, not while it is in electronic storage." *Id.* at 878. *See also* United States v. Steiger, 318 F.3d 1039, 1048-49 (11th Cir. 2003). In *Steiger*, the court stated "we hold that a contemporaneous interception-i.e., an acquisition during 'flight'—is required to implicate the Wiretap Act with respect to electronic communications."

[73] 135 F. Supp. 2d 623,628 (E.D. Pa. 2001).
[74] *Id.*
[75] *Id.* at 629,630.
[76] *Id.* at 630,631.
[77] *Id.* at 631.
[78] *Id.* at 632.
[79] *Id.* at 633.
[80] *Id.* at 634.

post-transmission storage."[81] Therefore, the court held that Nationwide had not violated the federal or state wiretap and stored communications statutes.[82]

Sometimes it is the employee who has intercepted the employer's e-mail messages. Even though the employer service provider has wide latitude in retrieving employee e-mail messages, there is no similar exception allowing employee retrieval of e-mail messages. However, in the following case, the employee could not be held liable under the Federal Wiretap Act because the e-mail messages were not intercepted during transmission.

In *Eagle Investment Systems Corporation* v. *Tamm*,[83] Tamm worked as a staff programmer for Eagle, with payments made to Tamm's company, Compendium Research Corporation, for Tamm's services. In April 2000 a dispute arose over a licensing fee that Tamm claimed Eagle owed. During the dispute, Tamm and Compendium sent Eagle a letter that had a copy of an e-mail attached to it. The October 17, 2000 e-mail was sent to Eagle's president and chief financial officer by Eagle's comptroller.[84]

Eagle sued Tamm alleging, among other things, that Tamm stole the October 17, 2000 e-mail in violation of the Federal Wiretap Act and the Stored Communications Act. Before the court was Eagle's motion to dismiss the claim under the Federal Wiretap Act.[85] Eagle acknowledged that Tamm acquired the October 17, 2000 e-mail after it was received by Eagle's president and chief financial officer. However, Eagle claimed that this acquisition was an interception prohibited by the Federal Wiretap Act. The court found that an interception had to occur during transmission of the e-mail. The court reasoned that if interception were interpreted to include access of e-mail during storage, then the remedy under the Federal Wiretap Act would duplicate the remedy under the federal Stored Communications Act. The court decided that Congress had not intended to provide duplicate remedies and dismissed Eagle's claim under the Federal Wiretap Act.[86]

Presumably, Tamm might be held liable under the Stored Communications Act. The court did not discuss the Stored Communications Act because Eagle's claim under the Stored Communications Act was not subject to the motion to dismiss.[87]

Case law in this section has shown that an employee has virtually no privacy with respect to the employee's e-mail messages where the employer is the service provider. Even if the third party is the one retrieving e-mail messages from storage, the remedies afforded by the federal statutes are fewer and to a lesser extent for e-mail messages than for oral and wire communications.

[81] *Id.* at 636.

[82] *Id.* at 637,638.

[83] 146 F. Supp. 2d 105,107 (D. Mass. 2001).

84 *Id.* at 107,108.

[85] *Id.*

86.at 112,113.

87.Id. at 107.

IV. TOWARD MORE PROTECTION FOR E-MAIL MESSAGES

It is much safer to telephone or send a letter than to e-mail someone. The letter, the telephone, and the e-mail are all methods of communication and all can be used to transmit the same message. However, the protection of the communication under the federal statutes depends on the method of communication used. Increased efficiency comes at a price. The same technology that allows e-mail messages to be transmitted quickly and at a low cost also allows someone to retrieve and read e-mail messages.

It is incongruous that the level of protection for private communication depends on the method of communication. The means of communication chosen results in disparate treatment for the communication. It is illogical that the most common means of communication, e-mail, has the lowest level of protection. Perhaps the least most common means of communication, a letter, is the most secure and receives that greatest level of protection.

The crucial time period for an oral or wire communication is while it is proceeding. In contrast, the crucial time period for an e-mail message is after transmission has been completed and when the recipient reads it. The Federal Wiretap Act and the Stored Communications Act provide a heightened level of protection to e-mail messages during the extremely short time period while the messages are in transmission and a lower level of protection after the e-mail messages have reached their destination. Because of the manner in which the e-mail messages are transmitted, it may be difficult for the e-mail messages to be intercepted while in transit. One e-mail message may be split into a number of electronic packets, each traveling by a distinct route, and the entire message being recompiled upon delivery at its destination. In addition, the transmission stage may last only a few minutes or less, while the time period during which the message is in storage at its destination may be hours, days, or weeks.

With e-mail communication becoming more and more prevalent, individuals are losing the privacy they once had. It was taken for granted that one's employer was generally not monitoring telephone conversations.[88] However, it is clear that e-mail messages, often a substitute for telephone calls today, may very well be monitored by one's employer.

Most employees have embraced e-mail communication wholeheartedly and its use is much greater than first imagined. Members of Congress certainly did not

[88] However, in certain situations the employer may legally monitor employee phone calls. Depending on applicable statutes, in some states the employer may monitor employee telephone calls either by using an extension telephone in the ordinary course of the employer's business or by securing the employee s consent in advance. CLIFFORD S. FISHMAN & ANNE T. MCKENNA, WIRETAPPING AND EAVESDROPPING §§ 7:3-7:10 (2d ed. Sept. 2002). The Federal Wiretap Act and the wiretapping and eavesdropping statutes of many states allow a telephone conversation to be recorded where one party to the conversation consents to the recording. However, a dozen or so states require all parties to the conversation to consent. In those states requiring all party consent, likely the other party to the conversation with the employee would also have to consent in advance. *See* Carol M. Bast, *What s Bugging You? Inconsistencies and Irrationalities of the Law of Eavesdropping,* 47 DEPAUL LAW REVIEW 837 (1998).

foresee use of e-mail communication as widespread as it is today when they added protection for electronic communication to the Federal Wiretap Act and the Stored Communications Act in 1986. With the ever-present use of e-mail as a prime method of communication, there is a threat to employee privacy that should be addressed by amendments to the Federal Wiretap Act and the Stored Communications Act.

The privacy one might expect for e-mail messages under the federal statutes is illusory. With many businesses providing e-mail service to their employees, those employees have little privacy. Generally, employees do not realize that employers may easily monitor the employees' e-mail messages. In most cases, the employer monitoring is lawful. The employer, as service provider, has virtually unlimited authority to access e-mail messages once they are in storage.

Electronic communication is treated differently from oral communication and wire communication in a number of ways.[89] First of all, there is no exclusionary remedy for the illegal interception of an electronic communication. This means that an illegally intercepted e-mail message can be used in court even though an illegally tape recorded face-to-face conversation or telephone conversation may not.

A face-to-face conversation can be tape recorded to store it. A telephone conversation can also be stored by tape recording it or by digitally storing it as an electronic communication. An electronic communication is stored in temporary and intermediate storage during transmission and is stored on a hard drive after transmission. Both an oral communication and a wire communication, once tape recorded, are protected under the Federal Wiretap Act; a stored electronic communication is only protected under the Stored Communication Act.

The distinction in levels of protection provided under the Federal Wiretap Act and the Stored Communications Act is important. The penalties under the

[89] Apparently when Congress amended the Federal Wiretap Act in 1986, the Department of Justice would not support equal treatment for electronic communication.

> According to Congressman Kastenmeier, only bills with Justice Department support had any chance of passage during the Reagan Administration, and the Department had made it quite clear that it believed electronic communication should be given a lower level of protection. In a hearing before the House Subcommittee on Courts, Civil Liberties, and the Administration of Justice, James Knapp, Deputy Assistant Attorney General for the Criminal Division, stated that the Department "believe(s) the interception of electronic mail should include some but not all of the procedural requirements of Title III." Specifically, he stated that the Department "strongly oppose[s] ... the inclusion of any new statutory exclusionary remedy." Knapp justified the Department's preference for a lower level of protection by stating that the "level of intrusion with aural communications is greater than the level of intrusion with electronic mail or computer transmissions." However, he also admitted that the Department wished to make interception "less burdensome on law enforcement authorities."

Michael S. Leib, *E-Mail and the Wiretap Laws: Why Congress Should Add Electronic Communication to Title Ill's Statutory Exclusionary Rule and Expressly Reject a "Good Faith " Exception,* 34 HARV. J. ON LEGIS. 393,410 (1997) (footnotes omitted).

Federal Wiretap Act are more severe than the penalties under the Stored Communications Act for a first offense. The civil remedies under the Federal Wiretap Act are more generous than the civil remedies under the Stored Communications Act. Law enforcement agents find it much more difficult to obtain a court order to intercept a communication under the Federal Wiretap Act than to obtain the warrant required under the Stored Communications Act. In addition, oral and wire communication obtained in violation of the Federal Wiretap Act can be excluded while there is no similar remedy for the illegal interception of an electronic communication or the illegal access to a stored electronic communication.

The Federal Wiretap Act and the Stored Communications Act should be amended to provide the same level of protection for e-mail messages that is now provided under the Federal Wiretap Act for face-to-face and telephone conversations.

V. CONCLUSION

There should not be a distinction in the level of privacy afforded an e-mail message in transmission and an e-mail message in storage. Because e-mail messages are as basic a means of communication as face-to-face conversations and telephone conversations, the same level of protection should be afforded e-mail messages, whether in transmission or in storage, as oral and wire communications. The Federal Wiretap Act should be amended to include stored electronic communication within the definition of electronic communication. With the Federal Wiretap Act thus amended, there would be no further need for the Stored Communications Act and those statutes could be repealed.