LEGAL RAMIFICATIONS OF ARCHIVED E-MAIL

Monica C. Holmes, Central Michigan University, monica.c.holmes@cmich.edu
Elizabeth A. Campbell, Central Michigan University, elizabeth.a.campbell@cmich.edu

ABSTRACT

The growing practice of archiving electronic communications is fraught with a myriad of heretofore unforeseen legal and information systems ramifications. Archived e-mail simply expands exposure of the communication. The purpose of this paper is to present an awareness of the potential liability for injuries suffered because of invasion of privacy or defamation arising from archiving (warehousing if you will) communications and to provide managers of information systems with recommendations regarding archiving practices.

Keywords: Email, legal, archives, liabilities, internet service providers

INTRODUCTION

Historically, the only dependable permanent records of communications were printed materials – written words, written symbols. With the coming of the postal service and the telephone, governments enacted laws that protect against the unauthorized access to communications. For example, letters sent by first class mail are stringently protected from public interception, access and disclosure. In fact, people also generally accept (1) that access to telephone is socially private and (2) that telephone companies would not be expected to monitor telephone usage [4].

However, these historic measures of legal protection have not kept pace with electronic communications, e.g., email [6] [14][18]. Letters can be shredded or burned before any third party reads them. An email may still exist somewhere after it has been deleted by the recipient. In a survey of workplace monitoring and surveillance by the American Management Association, over two thirds of the employers who responded monitor, archive and review employees' emails [2]. "E-mail is the day's evolutionary hybrid of traditional telephone communications and regular postal service mail" [16]. Employees are also not aware of the privacy issues involved in the use of workplace email [6]. Recent Federal legislation has been enacted to extend protections to electronic communications, but such measures have been weak and unclear, and have suffered confusing interpretations by the judicial system in their limited enforcement. To date, at the federal level, the 1986 Electronic Communications Privacy Act (ECPA) and the 1996 Communications Decency Act (CDA) are the only federal laws designed to address concerns regarding electronic communications. The proposed Privacy for Consumers and Workers Act (PCWA) has languished in Congressional Committees since 1991.

Similar to surface or postal mail, e-mail provides no direct transmission from sender to receiver. Instead, many intermediaries are involved in the delivery process [14]. First, the sender must access the system by "logging on". Once a message is composed and sent, the delivery provider places the message in temporary storage and makes a back-up of it for protection against crashes which may occur during transmission and before delivery. These two types of storage which occur up to this point are considered "pre-transmission storage." Once the recipient of the message opens it up and accesses it, the message is removed from the transmitter's intermediate

storage, and can then be placed in "post transmission storage". Received email is usually stored on tapes, disk drives, and CD-ROMs. The e-mail may remain stored indefinitely and can be easily retrieved and reviewed. Where e-mail is involved, the delivery provider is the Internet Service Provider (ISP) which fulfills a role similar to that of the United States Postal Service. However, unlike USPS, the ISP saves a copy of the message, both in the pre- and post-transmission storages, in the event of computer crashes. This article focuses on the "post transmission" storage of e-mail, also known as archived e-mail. A discussion of the laws regarding communications follows.

THE LAWS PERTAINING TO COMMUNICATIONS

The Federal Government has been concerned about the protection of electronic communications for more than 60 years. The impact of the telephone and electronic technologies have focused on the wire transmission of oral communications. In 1968, Congress enacted a wiretap law known as the Omnibus Crime Control and Safe Streets Act. Certain provisions of the law, especially those sections concerning government powers, were controversial, giving rise to numerous court cases testing the interpretation, implementation and constitutional limitations of the statute [24]. In 1986, Congress amended the statute to include the ECPA. The amendments were intended to afford protection to new forms of communications, especially electronic communications, developed by advanced technologies which had not been addressed in the 1968 Act. Next came the enactment of the 1996 CDA of 1996. The general scope and purpose of the Act regarding e-mail is to afford protection, not to the e-mail sender or recipient but rather to the transmitter, carrier, or the individual responsible for the warehousing of the message.

Title I of the ECPA is known as the Wiretap Act and Title II as the Stored Communications Act (SCA). Title I protects against unauthorized "interception" and "disclosure" of "electronic communications," providing for government charges for violations resulting in criminal penalties of fines and/or imprisonment for not more than five years. It allows for a private civil cause of action against a violator which can be brought within two years of discovery of the violation. The SCA protects against unauthorized "access" to "electronic communication while it is in electronic storage," providing criminal penalties of fines and/or imprisonment up to one year for commercial offenses and a civil cause of action against a violator.

The original and main intent of the 1996 CDA was essentially to prohibit obscene materials from the Internet. The portion of the statute which provided criminal remedies for network communications which were deemed offensive was invalidated by the U.S. Supreme Court as an unconstitutional regulation of free speech [21]. But, the CDA states that no provider or user of an interactive service will be liable for voluntarily taking action to restrict access or to provide content providers the means to restrict access to material that a provider considers obscene, lewd, lascivious, filthy, excessively violent, harassing or otherwise objectionable even if such material may be constitutionally protected. The Act defines "interactive computer service" as:

> "any information service system, or access software provider that provides or enables computer access by multiple users to a computer system, including specifically a service or system that provides access to the internet and such system operated or services offered by libraries or educational institutions" [1].

Many states have introduced legislation similar to the ECPA, but few give additional protection such as that which would be provided by the proposed Federal PCW Act. An interesting question could surface as to the pre-emption provisions contained in the Federal CDA if states were to provide protections that contravene the federal statutes or that allow tort liability for the very conduct granted immunity under the Federal Act. At least one court has held that the Federal CDA pre-empts state common-law tort actions [12]. The next section provides examples of how the statutes have been applied by courts.

JUDICIAL APPLICATIONS OF THE LAWS PERTAINING TO COMMUNICATIONS

Judicial decisions applying the Federal EPCA and the CDA raise issues concerning the protections and liabilities of employers who archive or store sent and received e-mail. In a recent case, an employee maintained a secure web site that required user identification to log in with a password, and a promise of confidentiality made by the site visitor. The employer illegally accessed the secured web site and learned of its derogatory contents. The Court held that there was potential violation of both the Wiretap Act and the Stored Communication Act because the employer violated the act by intercepting a secure communication while in the "pre-transmission" stage of communication. The court said, "It makes no more sense that a private message stored in a voice mailbox should be protected from interception, but the same words expressed in an e-mail stored in an electronic post office pending delivery should not" [15].

Later, another case was decided involving an insurance agent who was an exclusive independent contractor for the defendant, an insurance company. The agent sent derogatory e-mails, using computer equipment leased to him by his principal, the insurance company. The principal retrieved the sent messages from its own storage site, i.e., from its archives, and cancelled the agency agreement. The court determined that the message was retrieved from post transmission storage (archives) after it had been received by the recipient. Consequently. the court held that this type of messages were not protected by the federal laws and there was no violation of the Wiretap Act or SCA [13]. According to this decision, e-mail that has been archived in "post transmission" storage is not intended to be protected by the EPCA.

Case law applying the CDA is sparse. The most notorious situation involved AOL, the commercial service provider who, though repeatedly given notice of false and defamatory information contained on one of its anonymous bulletin boards, did too little too late to remove the messages. The Court, relying on the immunity provisions of the CDA, held the ISP immune as a publisher and as a distributor [25]. The essence of this decision is that an ISP is absolutely immune from liability for the content of messages while the messages are in pre-transmission storage. However, the case does not answer the question as to whether this immunity afforded by the CDA will extend to those messages which are archived, i.e., in post transmission.

In view of the conflicting opinions illustrated in the above cases in applying the EPCA and the uncertainty of the application of the CDA to archived e-mail, it is not clear if these federal statutes are intended to cover "post transmission" storage or archived e-mail. It is also uncertain if "post-transmission" storage or archived email enjoys the immunity protection of the CDA. The next section examines the situation from both perspectives of the two federal statutes.

LEGAL LIABILITY AND PROTECTIONS REGARDING ARCHIVED E-MAIL

From the courts' interpretations of the federal statutes, an employer who archives e-mail may access it without fear of violating a federal statute, either because the statutes do not cover archived e-mail once received by the recipient or because the communication is archived in the employer's own information system. The CDA also prescribes that an ISP that provides or enables computer access by multiple users to a computer system, will be immune from liability as a publisher or speaker for the content of messages sent by third parties while that message is in transmission.

The greatest concern of those who have studied these statutes focuses on the lack of protection for privacy and against defamation to those recipients of emails which are then archived. After all, unlike surface mail or content in hard copy that can be easily disposed of, the recipient of an e-mail which contains defamatory content about the recipient or has data of a private nature, cannot simply shred it. The recipient has no say in its retention or its disposal or how often it may be accessed or who will see it. If that email with its damaging content is archived, accessed and viewed by others, what recourse in law does the recipient have? If there is legal recourse, what can IT managers do to protect against such legal consequences?

Immunity from Liability Provided under CDA

Congress grants ISPs immunity from liability for contents in electronic communications in order to allow electronic commerce to develop. The cost of the Internet would be prohibitive if the law placed liability for defamation or invasion of privacy on those who provide internet service to the public. Besides, authors of defamatory materials remain subject to legal liability no matter what form of delivery was chosen for the defamation [7], [8], [11].

The immunities provided by the CDA actually give ISPs the same degree of protection that the legal doctrine of "qualified privilege" provides to telephone companies as common carriers. The older telephone cases demonstrate similar problems, sometimes with unexpected decisions from the lower courts. A case for defamation was brought against a telephone company, which had been notified that its equipment was being used to carry extremely harmful falsehoods. The majority of the intermediate appellate court, swayed by the injured plaintiff's plight, imposed liability on the phone company for its failure to stop the transmissions [3]. However, a strongly worded dissenting opinion of a judge from the intermediate appellate court stated that the case against the phone company should be dismissed on the basis that the phone company was protected against such legal actions because it enjoyed a "qualified privilege." On an appeal of the case to the highest state Court of Appeals, that dissenting opinion prevailed [4].

Actually, the "qualified privilege" available to telephone companies is what immunity is to ISPs today [17]. This "qualified privilege" highlights several important social policies, some pertaining to the rights of the individual and others to those of ISPs. The dissenting judge suggested that there might be liability on the telephone company if it had knowledge of the falsity [4]. But, even if the falsity or the defamatory nature of the content is known to the ISPs, the CDA now protects them. Court decisions have expanded immunity protections under the CDA to protect both publishers and distributors even if they knew of the defamatory contents.

Still, it must be recognized that immunities were put into place by Congress for a variety of reasons. One reason was to override certain judicial decisions that had held ISPs liable as publishers for contents in electronic communications where the ISPs had editorial control but had not exercised it [23]. Congress also wanted to give ISPs an incentive to edit contents without a fear by them of becoming liable as publishers. Of course, the reverse has happened. Now that the Court has held that ISPs have immunity from liability, both as publishers and distributors, the ISPs have no incentive to edit the contents of electronic communication because they are not liable for any part of those contents [25], [10].

The more important issue is whether an employer who provides "interactive computer service" and who then archives e-mail enjoys the immunity protection of the CDA when that "post transmission" stored e-mail is retrieved, read by third parties and the defamatory or private data reaches the eyes of those other than the original recipient. Then, an argument can be made that the employer becomes a publisher. If that is the case, and if the immunities of the statute do not apply to archived messages, then the employer should be aware of the possible consequences.

Exceptions to Liability Provided under ECPA

The ECPA affords protection against the unauthorized interception of electronic communications while in transmission, accessing of communications while in temporary storage during transmission, and disclosure of the contents. The statute allows for exceptions to these prohibitions, thus allowing an employer to access e-mail and not violate the Act. The three exceptions to the prohibitions against unauthorized interception, access, and disclosing contents of electronic communications established in ECPA are the consent exception, the business use exception, and the service provider exception.

If an employer monitors workplace activity by archiving e-mail and can demonstrate applicability of one of these exceptions, then an employee's complaint under ECPA for unlawful access, interception or disclosure of e-mail will fail. The only question remaining is whether the employer enjoys immunity under the CDA for disclosing the contents of archived e-mail.

The Consent Exception under ECPA

The consent exception appears to be the easiest exception to address, in part because the exception was first applied and well tested in telephone monitoring cases, and in part because the term "consent" is discussed in many historic legal contexts. Employers should be aware that consent requires full notice and knowledge, either expressed or implied, by the employee.

The Business Use Exception under the ECPA

The "business use" exception appears to be available for telephone or telegraph instruments furnished to the user by the employer or being used by the employer during the ordinary course of *its* business, and to allow the employer to intercept, disclose or use the communication.

The consensus is that in order to benefit from this exception, the employer monitoring of employee communications must be conducted in the ordinary course of business, arise out of and pertain to business activities and have a legitimate business interest or legal interest in the content (e.g. monitoring sexual harassment). A balance must be struck between the legitimate interest of the employer and the privacy interest of the employee [20]. The monitoring of the

content of purely private communications which fall outside the parameters of the business would not constitute an exception to the prohibition of the statute. However, monitoring private communications to learn the extensive use of the employer equipment and time, could be viewed as permissible and thus fit within the umbrella of the business use exception.

The Service Provider Exception under the ECPA

The EPCA is vague concerning the business use and service provider exceptions where e-mail is involved because an ISP can be one other than the employer [22]. The consensus is that most employers who are the providers of e-mail services will be exempt from EPCA liability, and thus may monitor, archive and access communications at will; the courts follows this majority view.

CONCLUSION & RECOMMENDATIONS

Many have repeatedly called for further protection against e-mail monitoring and archiving in the workplace. The PCWA has, in one form or another, been introduced into Congress at least three times since 1991, but to date, there has been no enactment of such legislation. Currently, employees enjoy few legal protections against the archiving, accessing and disclosing of e-mail communications by an employer. Even most public employees will find that the employer, as the ISP of electronic communication services, receives almost full protection through the exceptions provided in the federal statutes. In the private sector, not only are the employees' e-mail communications not protected from an employer, but most employees are "at will" and can be terminated without cause. At the same time, however, employers must also beware of the practice of archiving e-mail. There is uncertainty regarding terms within statutes and the scope of protection provided in the statutes is untested. There is also extensive debate concerning the lack of protection given to employees regarding issues concerning e-mail.

Since there are many good reasons why an employer should archive e-mail, the following recommendations are made:

1. Establish a written policy regarding the storage of e-mail.
2. Specify precisely:
    i. How the policy will be enforced.
    ii. The consequences for violation of the policy.
    iii. Who owns equipment.
    iv. What is or is not permissible use of employer equipment.
    v. What communications will be archived for context.
    vi. What communications will be archived for content.
    vii. How the archiving of email will be accomplished.
    viii. The conditions for accessing and retrieving archived email.
    ix. What is meant by "ordinary course of business."
    x. That a password is no assurance of privacy.
3. Communicate the policy in writing to employees.
4. Position the information systems equipment as a service provider to receive all statutory protections.

In the absence of a valid search warrant issued by a court, an employer is well advised not to access archived e-mail without the knowledge and consent of the employee and without providing the employee an opportunity to review the contents first. If the contents contain defamatory or private information regarding the employee, the employer may well be considered a publisher once the contents are available to be read by others.

REFERENCES

1. 47 U.S.C.S. @ 230 (f) (2).
2. American Management Association Survey. (2002). "Workplace Monitoring and Surveillance: Summary of Key Findings," available at http://www.Amanet.org/research/ on March 15.
3. *Anderson v. New York Telephone Co*, 42 A.D. 2d 151; 345 N.Y.S. 2d 740, 1973.
4. *Anderson v. New York Telephone Co*., 320 N.E. 2d 647, 1974.
5. Ballam, Deborah A. (2000). "Employment-at-Will: The Impending Death of a Doctrine," *American Business Law Journal*, Vol.37, No. 4, pp.653-687.
6. Barsook, Bruce and Terry Roemer. (1998). "Workplace E-Mail Raises Privacy Issues," *American City & County* 113(10), pp. 10.
7. *Ben Ezra, Weinstein & Co. v. American Online* 206 F 3d 980, 19th circ., 2000.
8. *Bochan v. LaFontaine* 68 F. Supp. 2d 692, U.S.D.C. e.d. Va., 1999.
9. *Bohach v. City of Reno*, 932 F. Supp. 1232, D. Nev., 1996.
10. *Blumenthal v. Drudge and AOL* 992 F. Supp. 44, U.S.D.C., District of Columbia, 1998.
11. *Carafano v. Metrosplash, Inc* 2002 U.S. Dist. Lexis 10614, Media L. Rep. 1577, U.S. D.C., Calif., 2002.
12. *Doe v. Am. Online, Inc*. 783 So. 2d 1010, 2001, Fl.
13. *Fraser v. Nationwide Mutual Ins. Co*., 135 F. Supp. 2d 623, E.D. Pa., March 2001.
14. Kimball, Nina J. (2002). "Employees and Employers Beware: the Perils of E-Mail." Available at http://www.kbmlaw.com/emaildoc.html on August 30.
15. *Konop v. Hawaiian Airlines*, 236 F. 3d 1035, 9th Circ., January 2001
16. *Lunney v. Prodigy Services Co*., 723 N.E. 2d, 539, N.Y. Appeals, 1999.
17. *Lunney v. Prodigy Services* 723 N.E. 2d 539, 1999
18. McIntosh, Dan. (2000). "E-monitoring@workplace.com: The Future of Communication Privacy in the Minnesota Private-Sector Workplace," 23 *Hamline Law Review*, pp. 539-544.
19. Muhl, Charles J. (2002). "The Employment-At-Will Doctrine: Three Major Exceptions." Available at http://www.bls.gov/opub/mlr/2001/01/art1full.pdf on August 30.
20. *O'Connor et. al v. Ortega* 480 U.S. 709.
21. *Reno v. ACLU* 521 U.S. 844, 1977.
22. Schnaitman, Peter. (2002). Comment, "Building a Community Through Workplace E-mail: The New Privacy Frontier," 5 *Mich. Telecomm. Tech. L. Rev*. 177 (1999), available at http://www.mttlr.org/achives/ on July 27.
23. *Stratton Oakmont, Inc. v. Prodigy Services Co*., 1995 New York Misc. Lexis 712
24. *U.S. v. One District Court Judge*, 407 U.S. 297, 1072
25. *Zeran v. American Online, Inc*., 129 F. 3d 327, 4th circ., 1997.
    For more discussion on privacy issues and federal statutes, and cases, visit: http://profs.lp.findlaw.com/privacy/index.html and http://findlaw.com.