UIC John Marshall Journal of Information Technology & Privacy Law

Volume 23
Issue 1 *Journal of Computer & Information Law - Fall 2004*
Article 2

Fall 2004

To: Client@Workplace.com: Privilege at Risk?, 23 J. Marshall J. Computer & Info. L. 75 (2004)

Dion Messer

TO: CLIENT@WORKPLACE.COM: PRIVILEGE AT RISK?

DION MESSER†

I. INTRODUCTION

One of the most efficient means for attorneys to communicate with clients is via e-mail, and e-mail is quickly replacing the use of phone calls as the preferred method of communication between attorneys and clients.[1] Furthermore, attorneys have embraced e-mail technology, and the American Bar Association (ABA) has endorsed this method of communication.[2] Each year, the ABA performs a technology survey to determine trends in the legal community.[3] The technology "snapshot" from April 4, 2003, a survey performed in late 2002, reveals that eighty percent of attorneys use e-mail one or more times per day, and an additional eleven percent use e-mail one to four times per week.[4] The top uses for e-mail are: routine correspondence with clients and colleagues, ninety-six percent; memos or briefs, sixty-four percent; and the status of cases with clients and colleagues, sixty-three percent.[5] Furthermore, fifty-four percent of attorneys have used e-mail discussion lists for work purposes.[6]

---

† Clerk to the Honorable William C. Bryson, Federal Circuit Court of Appeals. JD from the University of Texas School of Law, MS in Electrical Engineering from the University of Texas, BS in Electrical Engineering from New Mexico State University. Registered to practice in Texas, the PTO, the Federal Circuit Court of Appeals, and soon to be in California. Contact: ddmesser@oeng.com. More information on patents and publications at: http://www.oeng.com/pdf/MesserResume.pdf. Special thanks to John Meline for his tremendous help with the idea and initial draft, to Professor John Dzienkowski for his support and contributions, and to Charles Richter for everything else.

1. Amy M. Fulner Stevenson, Comment: Making a Wrong Turn on the Information Superhighway: Electronic Mail, The Attorney-ClientPrivilege and Inadvertent Disclosure, 26 Cap. U.L. Rev. 347, 347 (1997).

2. ABA Formal Op. 99-413 (available at http://www.abanet.org/cpr/fo99-413.html) (accessed Aug. 26, 2004) [hereinafter ABA Op.].

3. ABA Legal Technology Resource Center, http://www.lawtechnology.org (accessed Aug. 26, 2004).

4. Kathryn A. Thompson, ABA Legal Resource Center, Technology Snapshot: The Results Are In, http://www.lawtechnology.org/presentations/techshow2003/techshow2003_files/frame.htm slide 25 (accessed Aug. 26, 2004).

5. *Id.* at slide 26.

6. *Id.* at slide 27.

Hence, e-mail is an integral part of many attorneys' legal communications. Unfortunately, these e-mail communications may end up in the clients' employers' hands due to a growing phenomenon, workplace monitoring of employees' computer use.[7] This paper explores the effects of workplace monitoring on the privilege and confidentiality of attorney-client e-mail communications.

In December, 2003, the American Management Association released the results of a survey of over 1000 companies about e-mail and computer monitoring.[8] An astonishing fifty-two percent of the surveyed companies monitor their employees' e-mail and computer activity, compared to forty-seven percent in 2001.[9]

Twenty-two percent responded that they had terminated employees as a result of monitoring.[10] Courts ordered a startling fourteen percent of those companies to produce employee e-mail, up from nine percent in 2001.[11] In advance of any ABA or Congressional action on this issue, a prudent attorney should consider implementing some precautionary measures to protect his client from losing the privilege and confidentiality of e-mail correspondence that the client may read or send in the workplace and to protect himself in any subsequent malpractice suit in which his correspondence with his client has lost its privilege due to workplace monitoring.[12]

The International Data Corporation (IDC) reports that companies spend one hundred and thirty-nine million dollars on content oriented e-mail monitoring software in 2001 and projects that by 2006 the monitoring software sales market will be six hundred sixty-two million dollars.[13] The IDC also reports that e-mail monitoring software was the only software segment in 2002 that increased profits and revenue.[14] These

7. This paper neither endorses nor discusses the previously addressed issue of whether employers should be allowed to monitor employees; it simply discusses the effect of monitoring on attorney-client privilege and confidentiality. See Larry O. Natt Grantt, II, An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace, 8 Harv. J. Law & Tech 345, (1995), discussing the privacy of monitored e-mail and related concerns of workplace monitoring policies.

8. American Management Association, *2003 E-Mail Rules, Policies, and Practice Survey*, http://www.amanet.org/research/pdfs/E-mail_Policies_Practices.pdf (accessed Aug. 26, 2004). More than fifty percent of over 1000 companies monitor employee e-mail.

9. *Id.*

10. *Id.*

11. *Id.*

12. Nicholas Varchaver, *The Perils of E-Mail,* http://www.fortune.com/fortune/technology/articles/0,15114,418678,00.html, (accessed Aug. 26, 2004) [hereinafter *Perils*].

13. *Id.*

14. IDT, Worldwide Security Software Forecast Update and Analysis, 2002-2007, (available at http://www.idc.com/getdoc.jsp?containerId=30254 (accessed Sept. 9, 2004). See also Andrew Schulman, The Extent of Systematic Monitoring of Employee E-mail and Internet Use, http://www.sonic.net/~undoc/extent.htm (accessed Sept. 9, 2004).

statistics indicate that e-mail monitoring is prevalent and growing in the U.S. workplace.

Employers monitor employee e-mail for a variety of reasons from non-technical to technical.[15] Some employers monitor to increase employee efficiency and productivity.[16] They believe that when they monitor e-mail and computer activity they are deterring employees' personal e-mailing and "surfing." Nancy Flynn, executive director of the ePolicy Institute, discovered that ninety percent of employees surveyed nationwide used e-mail at work for personal business.[17] According to the U.S. Bureau of Labor Statistics, the personal use of e-mail at work costs American businesses about eighty-five billion dollars annually.[18] Apreo, a company that produces a game-blocking software program called *AntiGame*, recently reported that computer game playing by employees costs more than fifty billion dollars per year.[19] The testimonials by managers who have installed the *AntiGame* software attest to the savings of money and time they realized by preventing their employees from playing games.[20] Some experts think, however, that game playing is taking a back seat to websurfing as an even larger "time-wasting tool."[21] One opines:

> From an employer's perspective, having unmonitored Internet access on each desk is roughly the equivalent of installing a gazillion-channel television set for each employee. In part because of its sheer convenience, and in part because businesses tend to have faster Web access, employees are finding it difficult to resist the temptation to shop for presents, plan vacation, check out sports scores, trade stocks, buy and sell items on eBay, correspond with friends and family, read reviews, buy movie tickets, and so on. There were certainly noncomputer ways to do all of these things before the Internet; it's just that the Internet makes it so much easier and less immediately obvious to the employer.[22]

Employers also monitor e-mail to protect their public image.[23] They

15. A recently published book, *The Naked Employee: How Technology is Compromising Workplace Privacy*, by Frederick S. Lane III contains a comprehensive discussion of workplace monitoring and is a good first source for learning about the growing phenomenon. Frederick S. Lane III, *The Naked Employee: How Technology is Compromising Workplace Privacy* (AMACOM 2003) [hereinafter *Naked Employee*].

16. Corey A. Ciocchetti, *Monitoring Employee E-Mail: Efficient Workplaces vs. Employee Privacy*, 2001 Duke L. & Tech. Rev. 26 (2001) [hereinafter Ciocchetti].

17. Teresa M. Mcleavy, *"Many New Jersey Companies Track Employee's Internet Usage,"* The Record (New Jersey), (November 23, 2003).

18. *Id.*

19. *Naked Employee*, *supra* n. 14, at 15.

20. Steve Watkins, http://www.apreo.com/about.asp?view=testimonials&tid=1000003 (accessed May 2, 2004).

21. *Naked Employee*, *supra* n. 12, at 15-16.

22. *Id.* at 16.

23. Ciocchetti, *supra* n. 15, at 26.

want to prevent the situation where an employee sends an off-color or distasteful e-mail outside of the company, because it might offend clients and generally tarnish the employer's image.[24] Employers also monitor to increase workplace safety.[25] The Occupational Safety & Health Administration (OSHA) statistics show that 16,664 violent, non-fatal workplace assaults occurred in 1999, and 674 workplace murders occurred in 2000.[26] At least one expert believes that "workplace violence may be the biggest single contributor to reduced employee privacy."[27]

Employers monitor e-mail to prevent workplace harassment.[28] They do not want workers downloading or relaying pornographic images to other employees who might then have a harassment claim against the employer. Fifty percent of surveyed employees reported that they received "pornographic, sexist, or racist e-mail at work."[29] A full seventy percent of all porn traffic happens during the time of a normal workday, which strongly suggests that some of it must happen in the workplace.[30] Employers monitor to reduce litigation as a result of pornography on its computers and networks.[31] Consider some recent cases of such litigation: nine women sued John Deere in 2001 alleging that coworkers printed out pornography from the Internet while at work on company time and on company computers and printers; twenty-six women sued Smith Barney in 1996 alleging that there was pornography distributed over the company network; and several women co-workers sued Chevron for hostile e-mail, including the "Twenty-Five Reasons Beer Is Better Than Women" e-mail, that circulated on the company network.[32] Between 1992 and 1997, companies spent one billion dollars to settle such claims as reported by the magazine Treasury and Risk Management.[33] This figure does not include the related costs of litigation and attorney fees.[34]

Employers also monitor to protect their intellectual property.[35] They do not want employees intentionally or inadvertently leaking their secrets outside of the company. Gartner Group discovered that the loss

---

24. *Id.*

25. *Naked Employee*, *supra* n. 14, at 18.

26. *Id.*

27. *Id.*

28. Ciocchetti, *supra* n. 15, at 26.

29. Torsten Ove, *"Companies Deal with Issue of Web Surfing, personal E-Mail Usage at Work,"* Pittsburgh Post-Gazette (March 19, 2000).

30. *See generally*, http://www.benutec.com/spymypc.htm, http://www.cerberian.com/02 products _ abusestats. htm, http:// www. cisilion. com/ internet- misuse. htm, http:// www. e-surveiller.com/statistics.htm

31. *Naked Employee*, *supra* n. 14, at 16-17.

32. *Id.*

33. *Id.* at 17.

34. *Id.*

35. Ciocchetti, *supra* n. 15, at 26.

of business information from e-mail is over twenty-four billion dollars every year.[36] Some employers, such as stock brokers and health care firms, are required to monitor and archive e-mail by statute.[37] Employers also monitor to prevent sabotage by employees, such as the case in 1996 when Omega Engineering, Inc. fired employee Timothy Lloyd.[38] Lloyd, a network program designer, set a "time bomb" software program that detonated after he was gone and destroyed Omega's main databases.[39] The resulting monetary loss was over ten million dollars, and Omega had to lay off eighty of its employees.[40] Companies also monitor to prevent cyber terrorism: hacking by outsiders and viruses attached to incoming e-mail messages.[41] A Boston internet analyst firm, the Aberdeen Group, estimated that firms spent over seven billion dollars in 1999 to prevent cyber terrorism, and the cost would rise to seventeen billion dollars by last year.[42]

Finally, employers monitor their employee e-mail to protect their network capacity.[43] They want to prevent situations such as the one that occurred several years ago when an employee sent a blanket e-mail containing singing and dancing reindeer to all of his co-workers, who in turn forwarded it to all of their friends and family (some of whom were at other businesses).[44] The result was that networks across the country became completely incapacitated because the e-mail message content was so large and sent to so many people at the same time. Employees were unable to send or receive legitimate business e-mail time during the network incapacity. For this reason as well as the previously mentioned reasons, employers will continue and increase employee e-mail monitoring.

How does workplace monitoring affect attorney-client privilege? Attorney-client privilege is the privilege afforded to a client that protects certain communications he has with his attorney regarding his case, as codified in the Federal Rules of Evidence.[45] At the same time, attorneys

36. Raj Panesar, *EmployerRresponsibility vs. Employee Privacy,* http://www.itsecurity.com/papers/mime8.htm (accessed Sept. 8, 2004).

37. *Perils, supra* n. 12.

38. *Naked Employee, supra* n. 14, at 13.

39. *Id.*

40. *Id.*

41. *Id.* at 22.

42. *Id.*

43. Ciocchetti, *supra* n. 15, at 26.

44. This account is from memory and occurred while I was working as an engineer at Motorola in the early 1990's.

45. Fed. R. Evid. 501, "Except as otherwise required by the Constitution of the United States or provided by Act of Congress or in rules prescribed by the Supreme Court pursuant to statutory authority, the privilege of a witness, person, government, State, or political subdivision thereof shall be governed by the principles of the common law as they may be

are increasing their e-mail communications with their clients, employers are increasing and expanding employee e-mail and computer use monitoring.[46] Employers' workplace monitoring endangers the privileged nature of attorney-client e-mail communications if clients access their confidential e-mail at work. An attorney who relies on the ABA endorsement for e-mail communications may be stepping into an ethical trap as well.[47] He could be violating his ethical responsibility to maintain client confidentiality if he e-mails confidential information to his client's work e-mail address where his client's employer is monitoring the workplace.[48] He could also be in violation if he knows that his client is accessing a private e-mail account remotely from the client's employer's computer where that employer is monitoring employee computer activity and content.[49] If an attorney does not maintain client confidentiality, he may be disciplined by the State Bar, or a court may find him liable to his client in a legal malpractice lawsuit.[50] Although there has been extensive legal discourse on employee privacy issues related to workplace e-mail monitoring, there has been amazingly little mention of the problem of maintaining the privilege and confidentiality of e-mail communications.[51]

---

interpreted by the courts of the United States in the light of reason and experience. However, in civil actions and proceedings, with respect to an element of a claim or defense as to which State law supplies the rule of decision, the privilege of a witness, person, government, State, or political subdivision thereof shall be determined in accordance with State law."

46. *Perils, supra* n. 12.

47. ABA Op., *supra* n. 2.

48. Model R. Prof. Conduct 1.6 (ABA 1999).

> (a) A lawyer shall not reveal information relating to representation of a client unless the client consents after consultation, except for disclosures that are impliedly authorized in order to carry out the representation, and except as stated in paragraph (b).
>
> (b) A lawyer may reveal such information to the extent the lawyer reasonably believes necessary:
>
> (1) to prevent the client from committing a criminal act that the lawyer believes is likely to result in imminent death or substantial bodily harm; or
>
> (2) to establish a claim or defense on behalf of the lawyer in a controversy between the lawyer and the client, to establish a defense to a criminal charge or civil claim against the lawyer based upon conduct in which the client was involved, or to respond to allegations in any proceeding concerning the lawyer's representation of the client. *Id.*

49. *Id.*

50. John F. Sutton, Jr., John S. Dzienkowski, *Cases and Materials On The Study of Professional Responsibility*, 104-168 (West 1989).

51. A search of Lexis for "e-mail /s monitor! /s employ!" in the combined law review data base reveals that more than 150 articles have been written about employee rights to privacy in the workplace when their e-mail is monitored. Only 4 of those references mention attorney-client privilege at all, and then only in passing.

Workplace monitoring is not the only ethical problem that occurs when attorneys communicate with their clients by e-mail. E-mail users inadvertently disclose e-mail more frequently than other forms of communication.[52] For instance, just this past summer a clerk at a prestigious law firm in New York e-mailed the entire firm a now infamous communication he intended exclusively for a law school buddy.[53] While you need to hit only one key stroke to copy an entire firm on an e-mail message, with regular mail, you would have to make considerably more effort to address envelopes to those same recipients. Similarly, it would be almost impossible to include the entire firm on a confidential telephone conversation. While copying the firm on a client e-mail may not harm the client, copying the opposing party's attorney very well could and can be accomplished with a simple click of the "reply all" key instead of the "reply" key. Such misaddressed e-mail is a very common problem among e-mail users.[54]

This paper explores the effect on privilege and confidentiality of e-mail in light of workplace monitoring. It first explores the historical background of and the ABA's position on e-mail use. Next, it explains some technical details of e-mail transmissions and workplace monitoring. After laying this foundation, the paper analyzes the legal attorney-client privilege issues surrounding e-mail communications in light of workplace monitoring. Finally, it identifies four ways to solve the problems associated with e-mail communications.

II. AN INTRODUCTION TO E-MAIL AND THE ABA'S POSITION

A. THE ORIGINS OF THE INTERNET AND E-MAIL

The predecessor to e-mail was created in 1969 as a project funded by the Defense Advanced Research Projects Agency (DARPA) and was

52. *See* Peter Coffee, *Security's Language*, http://www.eweek.com/article2/0,1759,1036767,00.asp (last updated April 21, 2003) (discussing the growing need for software solutions to stop inadvertently addressed e-mail). See also Niesha Gates, E-mail Regrets, Sacramento Bee D1 (July 29, 2002) (discussing several incidents of inadvertently addressed e-mail, including one that almost cost an employee his job). See also Prradyna Johsi & Stephen Williams, ATT&T Talks Up Flat-Rate Plan, Newsday A56 (Feb. 7, 2002) (reporting that Cisco had to report its earnings earlier than it expected to avoid SEC penalties because it inadvertently sent an e-mail to a large group of employees disclosing the good quarter ahead of when it planned to make this information public).

53. Thomas Adcock, *Errant Summer Associate E-mail is Sign of Changed Job Market*, 229 N. Y. L. J.,.16 (June 20, 2003) (A summer law clerk sent a very uncomplimentary e-mail to all of the attorneys at Skadden, Arps, Slate, Meagher & Flom when he intended to send it just to a friend clerking at another firm. The e-mail contained derogatory remarks about partners in the firm, and discussed the amount of time the clerk was wasting rather than working).

54. *See Naked Employee*, *supra* n. 14.

called Advanced Research Projects Agency Network (ARPANET).[55] ARPANET was very popular with its small group of users, but because its use was limited to those researchers,.several other networks based on and connected to ARPANET appeared.[56] As time went on, more networks were created and connected to ARPANET.[57] In 1990 ARPANET was decommissioned, and what remained is the Internet as we now know it.[58]

In 1972 Ray Tomlinson, a DARPA researcher, wrote the first e-mail application for ARPANET called SNDMSG.[59] SNDMSG was followed by ELM, one of the first full-screen interactive e-mail programs in the 1980's.[60] Developers improved and created newer e-mail programs as e-mail's use exploded in the early 1990's.[61] E-mail was the most widely used application of ARPANET and remains the most used application of today's modern Internet.[62]

B. The Historical Background of the ABA's Current Position on the Use of E-mail With Clients

In 1986 the American Bar Association's Committee on Ethics and Professional Responsibility responded to the onslaught of e-mail correspondence by advising that "lawyers should not communicate over any sort of online network without being certain that the system was capable of confidential, reliable communication."[63] As a result of this opinion, many state Bar Associations began issuing opinions on e-mail that recommended encryption and client consent for e-mail correspondence be-

---

55. Kevin Johnson, *Internet E-mail Protocols: A Developer's Guide* 11 (Addison Wesley 2000) [hereinafter *Protocols*] (It is not true that former Vice President Al Gore invented the Internet).

56. *Id.* Usenet; it is now what is commonly known as news or Usenet news, and was originally created as a link between Duke University and the University of North Carolina at Chapel Hill. *Id.* BITNET (Because It's Time Network) was started at the City University of New York, and the only software required to participate in it was e-mail. *Id.* CSNET (Computer Science Network) connected the University of Delaware, Purdue University, the University of Wisconsin, and the RAND corporation to provide researches access to e-mail. *Id.*

57. *Id.*

58. *Id.*

59. *Id.*

60. *Id.*

61. *Id.* at 12.

62. *Id.* at 13.

63. ABA Standing Comm. on Lawyers' Responsibility for Client Protection, *Lawyers on Line: Ethical Perspectives in the Use of Telecomputer Communication,* (1986) at 67. Malvern U. Griffin & Aaron P. Maurer, NetEthics: Concerns Regarding E-mail and World Wide Web Use by Attorneys, 59 Ala. Law. 44, 46 (1998).

tween attorneys and clients.[64] Other states adopted the opposite approach and endorsed the use of unencrypted e-mail for attorney-client correspondence.[65]

In 1999, the ABA responded to these varied state opinions by adopting as its official position the full endorsement of the use of ordinary e-mail for professional legal communication:

> A lawyer may transmit information relating to the representation of a client by unencrypted e-mail sent over the Internet without violating the Model Rules of Professional Conduct because the mode of transmission affords a reasonable expectation of privacy from a technological and legal standpoint. The same privacy accorded U.S. and commercial mail, land-line telephonic transmissions, and facsimiles applies to Internet e-mail.[66]

The ABA based its opinion partly on the fact that e-mail is broken into small packets that each (technically) travels randomly from network machine to network machine before reaching its destination and is therefore more difficult to intercept during transmission than telephone calls or regular mail "based upon current technology and law as we are informed of it."[67] Unfortunately, the ABA's analogy is flawed, as e-mail is much more susceptible to *legal* interception at its *delivery point* than is regular mail (regardless of random packet transmission).[68] The next section of this paper explains e-mail transmission so as to underscore why the analogy between e-mail and mail may not be appropriate in light of workplace monitoring policies. The ABA partly based its opinions on the protections provided by the Electronic Communications Privacy Act (ECPA) of 1986.[69] Section IV B explains that employer interception of e-mail during consensual workplace monitoring is an exception to the ECPA's statutory privacy protection.[70]

As far as telephone transmissions are concerned, the courts have already established that a speaker waives the privilege of his conversation if he knows or reasonably should know that a disinterested third party is

---

64. South Carolina Bar, Advisory Op. 94-27 (1995), Iowa Supreme Court Board of Professional Ethics and Conduct, Op. No. 96-1 (1996). Both opinions stating that attorneys should use encryption in e-mail correspondence.

65. Illinois State Bar Association, Op. No. 96-10 (1996), Electronic Communications; Confidentiality of Client Information; Advertising and Solicitation; Kentucky Bar Association, May 16, 1997, Electronic Communications; Confidentiality of Client Information; Advertising and Solicitation. Both allowed attorneys to correspond with clients via e-mail without encryption.

66. ABA Op., *supra* n. 2.

67. *Id.*

68. *Protocols*, *supra* n. 54, at 115.

69. 18 U.S.C. 2510-2707 (2003).

70. 18 U.S.C. 2510-2707 (1)(b)(iv) (2003).

monitoring.[71] An employer can legally monitor a workplace call if it falls under the consent exception or the ordinary course of business exception to the ECPA, formerly the Wiretap Act.[72] While an e-mail message might be like a private telephone call that enjoys the privacy protection afforded by the ECPA, it is much like a monitored telephone call in the context of workplace monitoring of e-mail and will not remain privileged.

III. TECHNOLOGY

A. How E-mail Transmission Works

E-mail rarely travels directly from the sender's computer directly to the recipient's; instead, an e-mail message typically passes from network computer to network computer until it reaches its final destination.[73] A network computer is called a "server."[74] Specifically, nearly all e-mail is transferred by the Simple Mail Transport Protocol (SMTP), which is designed as a "store and forward" mechanism.[75] When the sender sends an e-mail, the message travels first to the sender's e-mail server.[76] The server parses and "encapsulates" the message in a data object consisting of the message "body" and an envelope.[77] After the server parses the message, the server evaluates the delivery address to determine if it is correct and it also performs a Domain Name Server (DNS) lookup to as-

71. *United States. v. Gray*, 71 Fed Appx. 485, 490 (6th Cir. 2003) (The court held that when a third party was listening on her own extension phone to a call, she was a disinterested third party whose "presence on the phone defeated the privilege."). See also *United States. v. Hernandez*, 441 F. 2d 157, 160 (5th Cir. 1971) (Quoting *Rathbun v. U.S.*, 355 U.S. 107, 111 (1957), the court held that "[e]ach party to a telephone conversation takes the risk that the other party may have an extension telephone and may allow another to overhear the conversation.").

72. 18 U.S.C. 2511(2)(d) (2003) ("It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent [emphasis added] to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State."); "Any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business [emphasis added] or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business." 18 U.S.C. 2510 (5), (a) (2003).

73. InfoWest Global Internet Services, Inc., *How Does E-mail Work?*, http://www.infowest.com/Support/FAQ/E-mail/FlexQuestion1023406452 (accessed Sept. 14, 2004).

74. The British Chambers of Commerce, *What is a Server and What Can it do?*, http://www.bcentral.co.uk/issues/technology/networks/whatserver.mspx (accessed Sept. 14, 2004).

75. *Protocols*, *supra* n. 54, at 72.

76. David E. Wood, *Programming Internet E-mail* 15 (O'Reilly Media, Inc. 1999).

77. *Id.* at 73.

certain where to deliver the message.[78] When the server is ready to send the message and the message reaches the top of the delivery queue, the server will decide which one of three possible actions to apply to the e-mail message: mailing, relaying, and forwarding.[79] In this context, "mailing" a message means delivering it directly to its destination.[80] A majority of e-mail messages, however, require relaying and forwarding due to the presence of security mechanisms such as firewalls that exist in nearly all organizations and businesses.[81] Relaying allows employers to read, filter, and log incoming and outbound e-mail messages.[82] Forwarding is similar to relaying except that the envelope information is modified before the e-mail message is relayed to another intermediate machine.[83] A user can typically access and read her e-mail before it is delivered to her home computer by viewing it remotely on her e-mail provider's computer. E-mail is stored on the provider's computer until either the user requests delivery to her own computer or deletes it from the provider's.

As noted earlier, the ABA's assumption that e-mail is not susceptible to interception and tampering is misinformed and therefore ill-founded. The ABA stated, "[b]ecause the specific route taken by each e-mail message through the labyrinth of phone lines and ISP's [Internet Service Provider] is random, it would be very difficult consistently to intercept more than a segment of a message by the same author."[84] In fact, it is relatively easy to intercept an e-mail message. One of the most obvious weaknesses of e-mail is the SMTP protocol and its lack of security features.[85] E-mail messages are nearly always transferred as plain text.[86] E-mail messages are broken down into "packets" before being transmitted, with each "packet" containing a header with the necessary destination information. Each packet then travels through the network to its final destination on a route determined by servers along the way.

The packets are directed by Mail Transfer Agents (MTAs) that depend on the DNS system for addressing and routing between MTAs.[87] Furthermore, this routing information rarely changes, meaning that

78. 76. *Protocols*, *supra* n. 54, at 80.

79. *Id.* at 103.

80. *Id.*

81. Internet.com, http://www.webopedia.com/TERM/f/firewall.html (accessed Sept. 14, 2004).

82. *Protocols*, *supra* n. 54, at 106.

83. *Id.* at 107.

84. ABA Op., *supra* n. 2.

85. *Protocols*, *supra* n. 54, at 115.

86. *Id.*

87. Joshua M. Masur, *Safety in Numbers: Revisiting the Risks to Client Confidences and Attorney-Client Privilege Posed by Internet Electronic Mail*, 14 Berkeley Tech. L. J. 1117, 1148 (1999) [hereinafter Masur].

each packet could actually travel along the same path as the other packets that complete the e-mail message.[88] Additionally, the e-mail traffic is exposed to interception, even though the individual packets of information in a single e-mail message may follow different paths between a given set of MTAs.[89] Mail traffic, therefore, can easily be captured and reassembled, whether inside the organization or between MTA's.[90]

In practice, furthermore, all of the packets of a given message are likely to travel the same route to the recipient.[91] That together with the relative stability of the Internet network would allow someone to intercept a message at any of the nodes along the route.[92] An interceptor need learn and "conquer" only one technology to compromise a node and intercept data. Cisco, a single manufacturer, makes the routers used in seventy-five percent of the Internet, and all of these routers employ the same hardware and software for security and routing.[93] Joshua Masur, an attorney specializing in internet litigation, did an empirical study of the routing of e-mail packets across the country for a period of one year and found no variance in the routing of packets sent in any given twenty-four hour period.[94] As a matter of fact, over that one-year period, packets traveled the same route fifty percent of the time.[95] A person who knows the address of the transmitting and receiving servers could easily discover the most likely route packets in a message will travel and intercept those packets.

B. How Workplace Monitoring Works

There are several methods of monitoring employee computer use, including packet sniffers, file searching, log file monitoring, and personal desktop monitoring.[96]

1. *Packet Sniffers*

Packet sniffers are programs designed to view all of the traffic over the network.[97] A packet sniffer looks at each packet as it passes through

88. *Id.*

89. *Id.* at 80.

90. Stuart McClure, et al., *Hacking Exposed*, at 419 (4th ed., McGraw-Hill Osborne 2003).

91. Masur, *supra* n. 85.

92. This paper does not deal with the various problems associated with intentional interception of e-mail messages but includes this discussion for the purpose of revealing that the ABA's position is based on technically inaccurate information.

93. Synergy Research Group, Inc., *Router Market Shaken by Shifts in Market Share*, http://srgresearch.com/store/press/3-3-03.html (accessed Aug. 26, 2004).

94. Masur, supra n. 85.

95. *Id.*

96. *Naked Employee, supra* n. 14, at 127-52.

97. *Id.* at 144.

the network, whether or not the packet is addressed to the particular computer on which the sniffer is running.[98] A sniffer on an end user's computer sees only traffic received by or sent from that computer, but a sniffer on a server (such as an employer's e-mail server) sees all of the data packets passing through that server.[99]

A packet sniffer program is designed or configured either to capture and store all packets passing through the network or to "filter" by examining each packet and storing only those that contain specific phrases or data as defined by the employer's network administrator.[100] In either case, the stored packets are available for the employer's subsequent inspection.[101]

A popular filtering program is *Websense*, developed by Websense, Inc. of San Diego, California.[102] Websense, Inc. claims over 17,500 customers, including such major employers as IBM, American Express, and General Motors.[103] Its software can intercept and block web requests to particular sites and can even generate reports describing how each employee spends his time on his computer.[104] A sniffer, whether filtering or not, might store packets from e-mail transmissions and, therefore, can compromise the privacy of those messages.

2. *File Searching*

According to surveys, four of ten employers periodically search the contents of their employee's' electronic files.[105] Most operating systems provide standard tools to search for files with particular names or extensions (e.g., "doc") or even for files containing particular words or phrases.[106] In addition, commercial tools such as *Mark I* provide similar capabilities.[107] Many of those tools allow network administrators to automate the searching of each employee's electronic files.[108] *AntiGame* by Adepro of Irvine, California is even more sophisticated in that it uses a program's "signature" to find copies of that program, even if an employee has changed the name of the program.[109] While originally developed to detect games, *AntiGame* now allows an employer to add its own list of

98. *Id*
99. *Id.*
100. *Id.*
101. *Naked Employee, supra* n. 14, at 144.
102. *Id.* at 145.
103. *Id.*
104. *Id.* at 145-46.
105. *Id.* at 130.
106. *Naked Employee, supra* n. 14, at 131.
107. *Id.* at 130.
108. *Id.* at 131.
109. *Id.* at 132.

banned programs.[110]

Since e-mail messages are typically retained in "sent" and "received" folders on the sending and receiving ends, respectively, those messages are subject to scrutiny through file searching.[111] Even if an employee deletes his copy of a sent or received message, an image of that message remains on the employee's machine, and commercial programs such as *EnCase* by Guidance Software of Pasadena, California can recover those deleted files.[112] Furthermore, in many workplaces, an e-mail server also retains a record of all messages sent and received by its employees, providing easy access for file searches.[113] In addition, many organizations archive the files of all internal computer systems daily and might retain those archives for months or even years.[114]

3. *Log File Monitoring*

A computer may contain log files that maintain lists of resources the computer's user has accessed.[115] For instance, a Web browser typically stores the Web sites visited by its user, and a network administrator can easily access that information.[116] Furthermore, to reduce access time and network traffic, Web browsers often retain visited pages in an internal cache that is also accessible to network administrators.[117]

As noted earlier, deleting a file does not actually remove it from the computer's hard drive. So, even if an employee finds and deletes log files and caches, those files may still be accessible by the employer.[118] As Frederick S. Lane III observes, "given the sheer amount of information available, it's not surprising that browser caches have become a particularly popular source of investigation for company managers, prosecutors, and litigation attorneys."[119]

---

110. *Id.* at 131.

111. *Naked Employee, supra* n. 14, at 139.

112. *Id.* at 136. See also Betty Ann Olmsted, *Electronic Media: Management and Litigation Issues When "Delete" Doesn't Mean Delete*, 63 Def. Couns. J. 523 (1996).

113. *Id.* at 139.

114. Consider the case of Oliver North and John Poindexter, who communicated with each other by e-mail on the network system at the National Security Council. They each deleted the e-mail correspondence from their own computer hard drives, but it was stored on back-up tapes that were allowed as evidence for use by prosecutors in the Iran-Contra investigation. Laurie Thomas Lee, *Watch Your E-mail! Employee E-Mail Monitoring and Privacy Law in the Age of the "Electronic Sweatshop,"* 28 John Marshall L. Rev. 139 (1994). Also, consider the Justice Department's recent anti-trust case against Microsoft in which it discovered incriminating Microsoft e-mail messages authored by Bill Gates. Sean Doherty, "The Rules of Record Keeping," Network Computing, November 1, 2002.

115. *Naked Employee, supra* n. 14, at 143.

116. *Id.*

117. *Id.* at 144.

118. *Id.* at 135.

119. *Id.* at 144.

4. *Personal Desktop Monitoring*

Employers can install monitoring software or "spyware" on an employee's computer that will record every keystroke the employee types.[120] The largest player in this software arena is *Investigator*, developed by WinWhatWhere of Kenniwick, Washington.[121] *Investigator* is capable of transmitting and/or storing to a file not only every single key stroke the user has made, but also each dialog box the user encounters and even an snapshot of the entire content of the user's display at time intervals selected by the employer.[122] It can send its data to an employer periodically or when it encounters certain words or phrases.[123]

While there are dozens of products that operate like *Investigator*, some take a less invasive approach. *The Survey Suite* from Scalable Software of Houston, Texas simply records the amount of time employees spend at various computer-based tasks.[124] Since *The Survey Suite* runs locally on the employee's machine but transmits its data to a central server when the computer user opens an external application, it is especially useful for monitoring employees working remotely (such as telecommuters).[125]

Alternatively, an employer can opt for hardware that monitors an employee's computer use. For example, e-bugging.com offers *PC Monitor*, a device an employer can install between an employee's keyboard and the keyboard port on the employee's computer.[126] Once installed, PC Monitor records every keystroke the employee types.[127] Simple surveillance cameras provide yet another form of monitoring in that they can record the contents of the employee's display.[128] The May 2004 issue of the Institute of Electrical and Electronic Engineers Spectrum magazine features new and upcoming digital video surveillance systems that allow employers to archive perfectly reproduced images of employee activity for any length of time desired![129] Images are wirelessly transmitted to a "video vault" at a remote location where the employer can access them at anytime from anywhere.[130] Some monitoring software even pro-

120. *Naked Employee, supra* n. 14, at 128.
121. *Id.*
122. *Id.*
123. *Id.* at 129.
124. *Id.*
125. *Naked Employee, supra* n. 14, at 129.
126. *Id.* at 146.
127. *Id.*
128. *Id.* at 147.
129. Alfred Rosenblatt, *Was that Slip and Fall for Real?* 18 IEEE Spectrum (May 2004). These systems are designed to protect employers from litigating "slip and fall" cases when they are not actually responsible for injuries. They also archive all other activity, such as computer use by employees.
130. *Id.*

vides support for video surveillance. *Investigator*, for example, can take photographs of a computer's user if the computer is equipped with a web cam.[131] Furthermore, with the advent of wireless keyboards and internet connections, devices that eavesdrop on such wireless conversations will undoubtedly spring up soon.[132]

While keystroke monitoring might pose little threat to incoming e-mail transmissions, it would certainly record the contents of any e-mail message the employee typed and sent to her attorney. Software and cameras that record the user's display, on the other hand, could readily store the content of incoming as well as outgoing e-mail messages.

IV. THE LEGAL CONSEQUENCES OF WORKPLACE MONITORING

A. E-MAIL DIFFERS FROM REGULAR MAIL

Regular mail goes from the sender to the recipient in a sealed envelope, and intermediate handlers do not normally open and copy it before sending it along. Regular mail is sent to the client at his residence in most cases, or to a post office box, but rarely to an employee's workplace to be read by the employer before reaching the employee.[133] The recipient has no way to access regular mail before it is delivered to its final destination. On the other hand, most clients can take delivery of their e-mail anywhere, including at their workplaces where their employers can intercept and read it before it reaches the employees. While there may be similarities regarding the difficulty of intercepting e-mail and mail during transmission, the ABA analogy of e-mail to regular mail breaks down precisely because of the existence of workplace monitoring policies that allow employers to read a client's e-mail when he takes delivery of it in the workplace.[134]

Furthermore, e-mail is typically stored and archived by a user's provider and may be stored and archived at any network machine it reaches during transmission. In one respect, e-mail is more like a postcard than a letter, because every network machine through which it passes reads the message. Employers also store and archive e-mail messages, and a user does not really remove an e-mail from her computer simply by click-

131. *Naked Employee, supra* n. 14, at 128.

132. *Naked Employee, supra* n. 14, at 147.

133. Even if it is sent by regular mail to an employee, it is unlikely that it will be opened by the employer before reaching the employee.

134. It is not the entire reason. Most businesses regularly archive information on their servers for back-up recovery. Employee e-mail can exist archived for years. Suppose the business is in a lawsuit and subject to discovery. The business will have to sort and inspect which e-mail is relevant and discoverable, and even if it did not regularly monitor employee e-mail, it would monitor it in this circumstance.

ing the delete button.[135] It remains on the computer hard drive until the computer needs that hard drive location again.[136] Therefore, multiple copies of the e-mail message are saved, even when the user deletes the message. Conversely, recipients of regular mail receive the only copy of the message the sender intended to send, and the recipient can reliably destroy the message.

B. E-MAIL INTERCEPTION IS ORDINARILY PROTECTED BY STATUTE

It is a Federal crime to intercept regular mail, and intercepted mail cannot be admitted as evidence in court proceedings.[137] The Electronic Communications Privacy Act (ECPA) of 1986 provides similar legal protection for intercepted e-mail. The ECPA makes the interception of an e-mail message by a third party a criminal act and protects the privilege afforded any illegally intercepted message.[138] As previously discussed, the ABA relied on the protection afforded by the ECPA in reaching its opinion that attorneys could communicate with clients by e-mail. The ECPA states that "[n]o otherwise privileged . . . electronic communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character."[139] Title I of the ECPA prohibits anyone who knows or has reason to know that he is illegally intercepting electronic communications from disclosing those communications.[140] Title I provides for actual damages and profits, as well as, both statutory and punitive damages.[141] Title II of the ECPA even protects access to stored communications but limits damages to actual damages or profits.[142] An attorney can count on the ECPA to protect the attorney-client privilege of illegally intercepted e-mail. This protection is a statutory protection and is outlined in § 2515, "Prohibition of use as evidence of intercepted wire or oral communications."[143] Section 2515

135. *See* Betty Ann Olmsted, *Electronic Media: Management and Litigation Issues When "Delete" Doesn't Mean Delete,* 63 Def. Couns. J. 447 (1996).

136. *See* James K. Leman, *"Litigating in Cyberspace" Discovery of Electronic Information,* 8 S. C. Law. 14, 15, (1997).

137. *See* 18 U.S.C. § 2515 (2004) (Prohibition of use as evidence of intercepted wire or oral communications. "Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter.").

138. 18 U.S.C. § 2511(1)(a) and (d) (2004).

139. 18 U.S.C. § 2517(4) (2004).

140. 18 U.S.C. § 2511(1)(a) and (d) (2004).

141. 18 U.S.C. § 2511(5) (2004).

142. 18 U.S.C. § 2701(a)(2) (2004).

143. 18 U.S.C. § 2515 (2004).

provides that "no part of the contents of such communication and no evidence derived therefrom may be received in evidence."[144]

C. WORKPLACE MONITORING OFTEN FALLS UNDER AN EXCEPTION TO THE STATUTE[145]

As discussed previously, an employer may legally monitor and record employee telephone conversations if it obtains the prior consent of the employee.[146] When an employee signs an employment agreement that allows his employer to own and monitor e-mail, computer transactions, and telephone calls on employer owned equipment, he gives up the statutory privacy protection afforded him by the ECPA. Under these circumstances, employer interception of the e-mail is no longer "in accordance with" or "in violation of" the ECPA and loses the immunity from discovery afforded by § 2517(4).

D. ATTORNEY-CLIENT COMMUNICATION

The client can expressly waive the attorney-client privilege.[147] Unfortunately, the client or attorney may inadvertently waive it by actions such as revealing the contents of privileged communications to parties without a need to know.[148] It is a well-established principle of law that a client waives the attorney-client privilege if he discloses the contents of a privileged communication to anyone who is not an interested party to the action.[149] This is true even if the disclosure is inadvertent.[150] An ad-

144. *Id.*

145. *See* Matthew J. Boettcher and Eric G. Tucciarone, Concerns Over Attorney-Client Communication Through E-Mail: Is the Sky Really Falling?, 2002 L. Rev. M.S.U.-D.C.L. 127 (2002). *See also* Masur, *supra* n. 85. *See also* Jeremy U. Blackowicz, E-Mail Disclosure To Third Parties in the Private Sector Workplace, 7 B. U. J. Sci. & Tech. L. 80 (2001).

146. 18 U.S.C. 2511(2)(d) (2004) ("It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State."); 18 U.S.C. 2510 (5) (2004) ("(a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business.")

147. Model R. of Prof. Conduct, Rule 1.6(b) (ABA 2003).

148. *United States v. Ryans*, 903 F.2d 731, 741 n. 13 (10th Cir. 1990) (A client can inadvertently waive privilege if a third party overhears a confidential conversation, for instance).

149. *United States v. Jones*, 696 F.2d 1069, 1072 (4th Cir. 1982) ("Any voluntary disclosure by the client to a third party waives the privilege.").

150. *Id.*

verse party can discover a waived communication that has lost its privilege and, provided the communication is relevant, use it in the courtroom during litigation.[151] Such an event can have a devastating effect on a client's case.[152]

In *Lewis v. UNUM Corp. Severence Plan*, corporate attorneys intentionally sent an e-mail message containing privileged information to members of the corporation who were neither necessary to the case nor in the top echelon of company management.[153] The court noted that it was the defendant's burden to establish that it did not waive privilege when the attorney sent the e-mail and ruled that it failed to meet its burden because "the substance of all of these otherwise privileged communications were intentionally disclosed to a third party."[154] The court held similarly in *Ocean Atl. Dev. Corp. v. Willow Tree Farm.*[155] The company sent an e-mail containing privileged information outside of a "control group" that consisted of those employees in top management and those in a position to act on the attorney's advice and then wanted to withhold the e-mail from discovery.[156] The court ruled that when the client e-mailed outside of its control group, it waived the privilege of the content of that e-mail.[157] The lesson from these two cases is that when a client or his attorney *intentionally* includes recipients who are outside the scope of the case, he waives the privileged nature of the e-mail.

E. WORKPLACE MONITORING IS ANALOGOUS TO INTENTIONAL INCLUSION

Suppose an attorney sends a privileged communication to an employee at her personal e-mail account and she opens it at work. Consider also that as a condition of employment, she signed a written contract agreeing that her employer could monitor her computer and could store and view anything on her computer display. Should courts consider the employer an "intentional recipient" because the employee agreed to workplace monitoring? Precedent in these largely uncharted waters suggests that the answer to this question is "yes," and the inquiry hinges on whether the employee had a reasonable expectation of e-mail and computer use privacy. The Supreme Court has held:

---

151. *See* Fed. R. Evid. 402 (2003).

152. For instance, if a judge orders an employer to produce all personal e-mail relevant to the employee's case, attorney-client communications discussing case strategy and other confidential information will be produced as well. The opposing party will have confidential information it would not otherwise be entitled to if the communications has been by regular mail.

153. *Lewis v. UNUM Corp. Severence Plan*, 203 F.R.D. 615, 621 (D. Kan. 2001).

154. *Id.*

155. 2002 U. S. Dist. Lexis 15841 (N.D. Ill. 2002).

156. *Id.*

157. *Id.*

> Because the reasonableness of an expectation of privacy, as well as the appropriate standard for a search, is understood to differ according to context, it is essential first to delineate the boundaries of the workplace context. The workplace includes those areas and items that are related to work and are generally within the employer's control. At a hospital, for example, the hallways, cafeteria, offices, desks, and file cabinets among other areas, are all part of the workplace. These areas remain part of the workplace context even if the employee has placed personal items in them, such as a photograph placed in a desk or a letter posted on an employee bulletin board.[158]

Accordingly, courts have pointed out in the following cases that when an employee knows his employer is monitoring his e-mail, he cannot have an expectation of privacy when he accesses confidential e-mail at work. For instance, the court in *United States v. Monroe* ruled that employees have no reasonable expectation of e-mail privacy when an employee using a federal government computer system to view child pornography wanted his e-mail suppressed.[159] The court emphasized that the employee was notified that "users logging on to this system consent to monitoring by the Hostadm" each time they logged onto the system.[160] The court concluded that the employee "had no reasonable expectation of privacy in his e-mail messages or e-mail box at least from the personnel charged with maintaining the EMH system," and it allowed the e-mail into evidence.[161] In *Garrity v. John Hancock Mutual Life Insurance Company*, the court ruled that an employee's e-mail is not private even when each employee created a personal mail folder protected by a password.[162] Some employees of John Hancock were using the company e-mail system to transmit and receive sexually explicit e-mail that a company policy specifically prohibited, and the company terminated them as a result.[163] They wanted the court to disallow the e-mail as evidence in their subsequent wrongful termination suit.[164] The court considered the fact that the employer had a written monitoring policy and that the employee had signed an agreement to abide by the policy when it ruled that the employees had no expectation of privacy.[165] The court allowed the e-mail into evidence.[166] The court also alternatively noted that even in the unlikely event that the employees could have established that they had a

158. *O'Connor v. Ortega*, 480 U.S. 709, 715-16 (1987).

159. *U.S. v. Monroe*, 52 M.J. 326, 330 (C.A.A.F. 2000).

160. *Id.*

161. *Id.*

162. *See generally, Garrity v. John Hancock Mut. Life Ins. Co.*, 2002 U.S. Dist. LEXIS 8343 (D. Mass. 2002).

163. *Id.* at 1-3.

164. *Id.*

165. *Id.*

166. *Id.*

reasonable expectation of privacy, "defendant's legitimate business interest in protecting its employees from harassment in the workplace would likely trump plaintiffs' privacy interests."[167]

This latter ruling suggests that employees have no expectation that their e-mail is private even in cases where there is not a monitoring policy known to the employee, provided that the employer is monitoring for a legitimate business reason. The language of the ECPA also supports this position, as it includes a statutory exception for interception of employee communications in the ordinary course of business.[168] The court in *Smyth v. The Pillsbury Co.* went a step further.[169] The employer had assured its employees that their e-mail was confidential but terminated an employee for sending unprofessional e-mail.[170] In the subsequent wrongful termination lawsuit, the court held that employees had no reasonable expectation of e-mail privacy, and "the company's interest in preventing inappropriate and unprofessional comments or even illegal activity over its e-mail system outweighs any privacy interests the employee may have in those comments."[171]

The courts indicate with these cases that they will find that employees do not have a reasonable expectation of privacy when using e-mail on their employers' systems. They also indicate that e-mail loses its privileged status because employees do not have an expectation of privacy, strongly implying that the employer is an 'intentional recipient" of confidential communications between attorneys and clients. As a result of all of these holdings, courts may allow opposing parties to discover e-mail.[172]

V. SOLUTIONS

What should the ABA or Congress do in light of the fact that e-mail really is different from mail and an employer can legally intercept it at a workplace as an exception to the ECPA? There seems to be a limited number of options: (1) the ABA could issue another opinion that prohibits attorneys from communicating with their clients by e-mail; (2) Congress could amend the ECPA to protect the privilege of monitored e-mail except in cases involving both the employer and employee; (3) the ABA could require that attorneys encrypt email to their clients; or (4) the ABA

167. *Garrity*, 2002 U.S. Dist. LEXIS 8343 at 1-3.

168. 18 U.S.C. §§ 2701(c)(1), 2510(5)(a) (2004).

169. *Smith v. Pillsbury Co.*, 914 F. Supp. 97 (E.D. Pa. 1996).

170. *Id.* at 98.

171. *Id.* at 101.

172. Interview with Larry Leibrock, the nation's foremost electronic discovery expert, on December 13, 2003 revealed that in the last four months the courts have allowed him to recover personal e-mail in each of the five cases he has been hired to assist with. He was able to recover all e-mail relevant to the case. *See also* http://www.eforensics.com.

could issue an opinion requiring that attorneys inform their clients of the potential risks of communicating by e-mail and prohibiting e-mail communication to an employer e-mail account.

A. Complete Prohibition

The ABA could issue an opinion that prohibits attorneys from communicating with their clients by e-mail. This solution has at least two problems: (1) attorneys use e-mail communications with their clients because it is cheaper and more efficient than regular mail or phone calls, and (2) this method of communication is so widespread that enforcing a prohibition would be impossible.

The client pays less because his attorney spends less time sending him e-mail than trying to reach him by telephone or drafting and sending a formal letter. Furthermore, when attorneys communicate with their clients by e-mail, they are able to respond to their clients' needs much more expediently than with any other method of communication. It is likely that clients would not want to forgo these advantages and would prefer to risk losing privilege than discontinuing e-mail communications.

Authorities have had a very difficult time curbing and enforcing prohibitions on electronic transactions that are in widespread use by the public. Consider the case of Napster and music file-sharing.[173] Despite the fact that Congress enacted legislation making it illegal to share copyrighted music and courts enforce the legislation, the practice is still in use and popular with the public.[174] If the ABA prohibited e-mail communication between attorneys and clients, it is likely to face the same type of enforcement problems that exist with file sharing.

B. ECPA Amendment

Congress could amend the ECPA to protect the privilege of monitored e-mail except in suits involving both the employer and employee. Employers who monitor employees' e-mail for "legitimate business purposes" would be prohibited from releasing e-mail for employees involved in outside litigation but would still be able to use monitored employee e-mail in suits between both employer and employee.

Currently the ECPA only applies to and protects employees and others from someone intercepting their e-mail without their agreement and when employers are not monitoring during the "ordinary course of

173. Mark Landler, *Fight Against Illegal File Sharing Is Moving Overseas* W 1 The New York, N.Y. Times W1 (March 31, 2004).

174. *Id.*

business."[175] If Congress amended the ECPA to change "in accordance with" and "in violation of" to include "as an exception to," employees who have agreed that their employers own and can intercept their e-mail would be protected.[176] If an employee agrees to e-mail ownership and monitoring as a condition of employment or of use of his employer's computer system, this statutory change to the ECPA would protect the confidentiality of his e-mail. It is unlikely that a business-friendly Congress will make such a trespass on the rights of most employers.[177]

C. Encryption

The ABA could fall back to its initial opinion on attorney-client communications by e-mail and require that an attorney encrypt e-mail to his clients.[178] This would provide a solution in cases where an employer does not monitor the client's display contents but would be of little use in the more likely case that the employer is monitoring the contents of the client's display.[179] Once the client decrypts the e-mail and displays it on his screen, the employer has access to the decrypted contents of the confidential message. Additionally, encryption adds another level of computer complexity that the public typically resists. This solution also requires that both the client and attorney purchase additional software to encrypt and decrypt messages. The ABA could expect just as much resistance to this decision as to a complete prohibition.

D. Requirement of Precaution

The ABA could issue a revised opinion on attorney-client e-mail communications requiring that an attorney warn his client of the risks inherent with confidential e-mail communications and prohibiting confidential e-mail transmissions to and from a client's employer e-mail address. While clients might still access their personal e-mail from their employers' computers, they would do so knowing that they might be waiving privilege. Informing his client of the risk that the client might

175. The case law discussed in this note indicates that courts are giving "ordinary course of business" a very broad interpretation. As a result, the ECPA probably does not protect any employees in workplace monitoring situations.

176. 18 U.S.C. § 2517(4) (2003) (Stating "[n]o otherwise privileged . . . electronic communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character").

177. *2003 E-Mail Rules, Policies, and Practice Survey*, http://www.amanet.org/research/pdfs/E-mail_Policies_Practices.pdf (accessed Aug. 26, 2004) (More than fifty percent of over 1000 companies monitor employee e-mail).

178. *American Libraries Assoc. v. Pataki*, 969 F. Supp. 160 (S. D. N.Y. 1997) (The judge pointed out that many jurisdictions initially approved attorney client e-mail communications only if they were encrypted).

179. *Perils*, *supra* n. 12 (Varchaver points out that manufacturers of monitoring software are projecting phenomenal growth through 2006).

waive privilege would protect the attorney in any subsequent related malpractice actions by his client. It is possible that clients would find alternate ways of accessing their personal e-mail from their workplace that their employer cannot legally monitor, such as from their personal cell phones, pagers, or PDAs.

If the ABA issued this opinion, it would be placing additional burdens on attorneys. First, attorneys would have to learn to recognize employer e-mail addresses and refuse to use them. Second, they would also have to warn their clients about the potential risks of workplace monitoring. Third, since some clients have only their employer e-mail address, attorneys would have to know where to direct their clients to get secure personal e-mail addresses.

VI. CONCLUSION

Along with the rest of the business world, the legal community is expanding its use of e-mail in its conduct of business. It is unlikely to discontinue e-mail communication with clients. The ABA has endorsed e-mail communication due largely to its belief that unauthorized third parties would be unable to intercept e-mail transmissions, and because it believed that the ECPA provided protection to keep e-mail private. A problem it did not consider, however, is a client's election to read his e-mail at a workplace in which the client's employer is monitoring its employees' computer use. Many employer-employee work agreements state explicitly that the employer has a right to monitor all use of the employer's computer equipment, and the number of employers engaging in such monitoring is rising.

Employers are unlikely to stop workplace monitoring for the reasons discussed in the introduction. As a matter of fact, the statistics show an in increase in employer workplace monitoring. While the ECPA protects the privacy of most e-mail communications, an employer's monitoring of employee e-mail is an exception. Therefore, an employee who consents to workplace monitoring sacrifices the statutory protection of privacy of his e-mail afforded by the ECPA.

Courts have ruled that such e-mail communication is not privileged and therefore is subject to discovery. In some cases, courts have found that when an attorney sends e-mail to individuals in the same company but not directly related to the matter at hand, that e-mail loses its privilege. Perhaps more significantly, courts have ruled that workplace monitoring is analogous to intentional inclusion of third parties, that an employee has no expectation of privacy when reading e-mail at work, even when the employee did not consent to monitoring, and that an employer's legitimate business needs take priority over an employee's privacy interests.

At least four possible solutions exist. The ABA could prohibit attorneys from communicating with clients by e-mail. E-mail is more efficient that regular mail or telephone communications, however, and such a prohibition would be impossible to enforce. Congress could amend the ECPA so that it protects the privacy of employer-monitored e-mail. To have a significant effect, however, the amendment would have to provide protection in cases in which the employee has consented to monitoring, and such a step seems unlikely. The ABA could require that attorneys and clients encrypt e-mail their messages to one another. This requires additional software and effort and would not protect employees from all forms of monitoring. The ABA could require that attorneys warn clients of the risks inherent in reading e-mail at work and prohibit attorneys from knowingly sending e-mail to a client's workplace. This seems to be the most practical approach.

In advance of any ABA or Congressional action on this issue, a prudent attorney should consider implementing some precautionary measures to protect his client from losing the privilege and confidentiality of e-mail correspondence that the client may read or send in the workplace and to protect himself in any subsequent malpractice suit in which his correspondence with his client has lost its privilege due to workplace monitoring.