Missouri Law Review

Volume 66
Issue 4 *Fall 2001*

Article 2

Fall 2001

Fitting a Square Peg into a Round Hole: The Application of Traditional Rules of Law to Modern Technological Advancements in the Workplace

Gregory I. Rasin

Joseph P. Moan

Fitting a Square Peg into a Round Hole: The Application of Traditional Rules of Law to Modern Technological Advancements in the Workplace

Gregory I. Rasin[*]
Joseph P. Moan[**]

I. INTRODUCTION

In the ever-changing technological environment, the transmission of information has become as simple and as quick as the click of a mouse or the touch of a button. However, the emergence and widespread use of computers, electronic mail ("e-mail"), and the Internet in the workplace also has created challenges for employers, their attorneys, and the courts. Specifically, the courts are forced to apply traditional rules of law to modern technological advancements. The lack of symmetry between these two notions has created uncertainty for today's employer. This Article discusses the impact of new technology on employment law, particularly in the areas of the discovery process, employer liability for employees' electronic communications, and the attorney-client privilege.

---

* Gregory I. Rasin is a senior partner at Jackson Lewis Schnitzler & Krupman and heads the firm's litigation department nationwide.

** Joseph P. Moan was Senior Counsel at Texaco, Inc., and is currently counsel at Jackson Lewis Schnitzler & Krupman.

II. THE IMPACT OF NEW TECHNOLOGY ON THE DISCOVERY PROCESS

At its essence, the discovery process seeks to compel the opposing party in civil litigation to produce information that could be damaging to his or her case. Rule 34(a) of the Federal Rules of Civil Procedure governs the scope of this process. In 1970, Rule 34(a) was amended to provide for the discovery of "data compilations from which information can be obtained [or] translated if necessary, by the respondent through detection devices into reasonably usable form."[1] The amendment also allows for the inspection, testing, copying, or sampling of "any tangible things which constitute or contain matters within the scope of Rule 26(b)."[2] Although the language of the 1970 amendment is somewhat cryptic, the notes from the 1970 Advisory Committee make clear that the revision was made "to accord with changing technology."[3]

Since the 1970 amendment, and in accordance with the Advisory Committee's intention, courts consistently have held that electronic communications and information are discoverable under Rule 34(a).[4] Both plaintiffs and defendants, alike, have been ordered to produce computerized information, including e-mail,[5] employee data information, word processing documents,[6] and, in some instances, the computer itself.[7] Notwithstanding that

---

1. FED. R. CIV. P. 34(a).

2. FED. R. CIV. P. 34(a). Rule 26(b)(1), as amended in December 2000, provides: "Parties may obtain discovery regarding any matter, not privileged, that is relevant to the claim or defense of any party, including the existence, description, nature, custody, condition, and location of any books, documents, or other tangible things. . . ."

3. Bills v. Kennecott Corp., 108 F.R.D. 459, 461 (D. Utah 1985).

4. *See, e.g.*, Sattar v. Motorola, 138 F.3d 1164, 1171 (7th Cir. 1998) (allowing the discovery of 210,000 pages worth of e-mails in a religious discrimination claim); *In re* Brand Name Prescription Drugs Antitrust Litig., Nos. 94 Civ. 897 & MDL 997, 1995 WL 360526, at *1 (N.D. Ill. June 15, 1995) (enforcing an e-mail discovery request); *Bills*, 108 F.R.D. at 461 (ordering the production "of documents containing detailed, particular information regarding numerous employees at [the defendant's] Utah operations" in an age discrimination case).

5. Discovery requests seeking a litigant's electronic mail ("e-mail") have become commonplace. Attorneys consider e-mail a potentially wealthy source of discovery because e-mail messages are often written very informally. As a result, each time an e-mail message is sent, the computer user unwittingly may have created a potentially discoverable document for future litigation. For a discussion of how e-mail messages, and other technological advancements, can expose an employer to liability, see *infra* notes 82-157 and accompanying text.

6. *See Sattar*, 138 F.3d at 1171; Simon Property Group L.P. v. mySimon, Inc., 194 F.R.D. 639, 641 (S.D. Ind. 2000); Easley, McCaleb & Assocs., Inc. v. Perry, No. E-2663 (Ga. Super. Ct. July 13, 1994). For example, the District Court for the District of Utah stated:

In many instances it will be essential for the discovering party to know the

"today it is black letter law that computerized data is discoverable if relevant," many issues remain.[8] Does the term "data compilation" include documents and electronic communications that the computer user seemingly "deleted" yet persistently survive on the computer's hard drive? May a litigant produce such discovery on computer disk, or must the documents be produced in hard copy? Finally, who bears the expenses in producing the electronic discovery? "[B]ecause we live in a society which emphasizes both computer technology and litigation," employers must familiarize themselves with these issues to prevent future liability.[9]

A. The Manner in Which Electronic Information Is Produced

In 1980, Rule 34 was amended to require parties to produce documents for inspection "as they are kept in the usual course of business or . . . organize and label them to correspond with the categories in the request."[10] The dual intentions of this requirement are to prevent a respondent from "deliberately . . . mix[ing] critical documents with others in the hope of obscuring significance"[11] and to provide the requesting party with documents in usable form.[12] In the context of electronic discovery, however, the latter purpose may be frustrated because parties often do not have identical computer programs that would allow them to review responsive computerized information. Eerily anticipating this scenario, the 1970 amendments to Rule 34 provide that when producing data compilations, the respondent may be required to translate such information through detection

---

> underlying theory and the procedures employed in preparing and storing the machine-readable records. When this is true, litigants should be allowed to discover any material relating to the record holder's computer hardware, the programming techniques employed in connection with the relevant data, the principles governing the structure of the data, and the operation of the data processing system.

Bills, 108 F.R.D. at 461.

7. *See* Ill. Tool Works, Inc. v. Metro Mark Prods. Ltd., 43 F. Supp. 2d 951, 954 (N.D. Ill. 1999); *cf.* Fennell v. First Step Designs, Ltd., 83 F.3d 526, 533 (1st Cir. 1996) (holding that the district court did not abuse its discretion in refusing to permit the plaintiff to access the defendant's hard drive).

8. Anti-Monopoly, Inc. v. Hasbro, Inc., No. 94 Civ. 2120, 1995 U.S. Dist. LEXIS 16355, at *4 (S.D.N.Y. Nov. 3, 1995); *see Bills*, 108 F.R.D. at 461 ("It is now axiomatic that electronically stored information is discoverable under Rule 34. . . .").

9. *Bills*, 108 F.R.D. at 461.

10. FED. R. CIV. P. 34(b).

11. FED. R. CIV. P. 34(b) advisory committee's note.

12. *See* FED. R. CIV. P. 34(a).

devices so as to produce the information in usable form.[13] The Advisory Committee to the 1970 amendments clarified the requirement by stating:

> [W]hen the data can as a practical matter be made usable by the discovering party only through respondent's devices, respondent may be required to use his devices to translate the data into usable form. In many instances, this means that respondent will have to supply a printout of computer data.
>
> . . . .
>
> [Similarly, if] the discovering party needs to check the electronic source itself, the court may [so order].[14]

Although there is little case law addressing the 1970 and 1980 amendments in the context of the manner in which electronic discovery must be produced, the holdings of those courts that have discussed the issue illustrate that their approach to electronic discovery has progressed over time. As the use of advanced technological communication and computer document storage devices become commonplace, it appears that the courts have become more amenable to discovery requests seeking information in computerized form.

For example, in the 1982 case of *Williams v. Owens-Illinois, Inc.*,[15] the Ninth Circuit addressed a request for the production of computer tapes.[16] In *Williams*, an employment discrimination case and one of the earliest opinions addressing the manner in which responsive electronic information is to be produced, the trial court ordered the discovery of the information contained on the defendant's computer tapes through hard copy wage cards.[17] The court, however, did not order the defendant to turn over physical possession of the tapes.[18] In affirming the trial court's holding, the Ninth Circuit rejected the plaintiff's argument that this manner of discovery was inadequate.[19] The court stated: "While using the cards may be more time consuming, difficult and expensive, these reasons, of themselves, do not show that the trial judge abused his discretion in denying [the plaintiffs] the tapes."[20]

---

13. *See* FED. R. CIV. P. 34(a).
14. *Bills*, 108 F.R.D. at 461-62.
15. 665 F.2d 918 (9th Cir. 1982).
16. *Id.* at 932-33.
17. *Id.*
18. *Id.*
19. *Id.*
20. *Id.* at 933.

In 1995, the United States District Court for the Southern District of New York reached a contrary conclusion in *Anti-Monopoly, Inc. v. Hasbro, Inc.*[21] In *Hasbro*, the plaintiff moved to compel the production of the defendant's data processing files.[22] The defendant objected to the production on two grounds: (1) that the information sought had been produced in hard copy format; and (2) that the defendant would have to create a computer program to retrieve and compile the information from its files, a time consuming and costly endeavor.[23] Notwithstanding the defendant's plausible arguments and the reality that the plaintiff's request would impose substantial costs upon the defendant, the district court held that "the law is clear that data in computerized form is discoverable even if paper 'hard copies' of the information have been produced, and that the producing party can be required to design a computer program to extract the data from its computerized business records."[24]

Three years later, the Seventh Circuit, in *Sattar v. Motorola*,[25] adopted an entirely different approach than that taken in the earlier *Williams* and *Hasbro* decisions. The *Sattar* case involved a race discrimination claim brought under Title VII of the Civil Rights Act of 1964.[26] At the trial level, the plaintiff sought production of more than 210,000 pages of e-mail in hard copy form.[27] The defendant had produced the e-mails.[28] However, production was in the form of non-conventional computer tapes.[29] The information was inaccessible to the plaintiff because he lacked the requisite equipment and software to review the tapes.[30] To resolve the discovery dispute, the trial court's order provided the defendant with the option of either downloading the e-mails on conventional computer disks or providing the plaintiff with the necessary equipment to review the information.[31] The defendant downloaded the e-mails onto a computer hard drive that it then loaned to the plaintiff for review.[32] The Seventh Circuit affirmed the trial court's approach and found it to be "an entirely reasonable resolution of [the plaintiff's] problem."[33] The evolution of the courts' resolutions of discovery

21. No. 94 Civ. 2120, 1995 U.S. Dist. LEXIS 16355, at *1 (S.D.N.Y. Nov. 3, 1995).

22. *Id.*

23. *Id.*

24. *Id.*

25. 138 F.3d 1164 (7th Cir. 1998).

26. *Id.* at 1166.

27. *Id.* at 1171.

28. *Id.*

29. *Id.*

30. *Id.*

31. *Id.*

32. *Id.*

33. *Id. But see* Fennell v. First Steps Designs, Ltd., 83 F.3d 526 (1st Cir. 1996). In *Fennel*, the plaintiff sued the defendant, the plaintiff's employer, alleging that the

disputes involving electronic information not only demonstrates the courts' attempt to embrace this new form of discovery, but also it illustrates that a litigant's uncertainty in this area is primarily caused by the courts' dilemma in applying old rules to new issues of law.

B. The Cost of Producing Computerized Information

Setting aside the uncertainty a litigant faces as to the proper form of producing electronic discovery, the respondent to a discovery request also faces economic uncertainties—such as, who pays for the production? Generally, the respondent bears the cost of gathering and reviewing responsive documents, while the requesting party bears the cost of copying such documents.[34] Rules 34 and 26(b), however, permit courts to shift the costs of production between the parties upon a showing of "undue burden or expense."[35] The interaction of these rules grants courts the power to shift the financial burden of discovery where the courts, in their discretion, deem appropriate.[36] In making this determination, courts will weigh the benefits and burdens of the discovery and "consider the needs of the case, . . . the importance of the issues at stake, the potential for finding relevant material and the importance of the proposed discovery in resolving the issues."[37] However, the application of this balancing test to the production of electronic discovery raises novel issues, primarily because the costs associated with producing electronically stored data are often far more excessive than the costs of producing "traditional" written materials.[38] Is a respondent required to pay for the creation of a computer retrieval program? Does a court impose an undue burden on the requesting party in requiring it to pay for the copying of hundreds of thousands of e-mails, in addition to the copying of respondent's written discovery materials? As with the manner of production of computerized information, courts

---

defendant discharged the plaintiff in retaliation for reporting a sexual harassment complaint. *Id.* at 528. The plaintiff sought access to the defendant's hard drive to determine whether the defendant was fabricating employee data. *See id.* at 532-33. The First Circuit affirmed the district court's ruling denying the plaintiff access to the defendant's computer. *See id.* The court noted that the plaintiff's discovery request would involve great risks and costs, including the risk of permanently affecting the defendant's hard drive and network system. *Id.* at 533 n.8.

34. *See* Hon. Shira A. Scheindlin & Jeffrey Rabkin, *Electronic Discovery in Federal Civil Litigation: Is Rule 34 Up to the Task?*, 41 B.C. L. REV. 327, 356 (2000).

35. FED. R. CIV. P. 26(b).

36. *See* Oppenheimer Fund, Inc. v. Sanders, 437 U.S. 340, 362-63 (1978).

37. Playboy Enters. v. Welles, 60 F. Supp. 2d 1050, 1054 (S.D. Cal. 1999) (citing FED. R. CIV. P. 26(b)(2)).

38. *See* Corinne L. Giacobbe, Note, *Allocating Discovery Costs in the Computer Age: Deciding Who Should Bear the Costs of Discovery of Electronically Stored Data*, 57 WASH. & LEE L. REV. 257, 262-65 (2000).

have failed to agree on who should bear the costs of producing electronic information.

The conflict appears to arise from the hesitancy of some courts to deviate from the framework of discovery in civil litigation by shifting the costs of gathering and reviewing responsive electronic discovery onto the requesting party. For example, in *In re Brand Name Prescription Drugs Antitrust Litigation*,[39] the court noted that:

> [i]t would be a dangerous development in the law if new techniques for easing the use of information became a hindrance to discovery or disclosure in litigation. The use of excessive technical distinctions is inconsistent with the guiding principle that information which is stored, used, or transmitted in new forms should be available through discovery with the same openness as traditional forms. The normal and reasonable translation of electronic data into a form usable by the discovering party should be the ordinary and foreseeable burden of a respondent in the absence of a showing of extraordinary hardship.[40]

Notwithstanding that the cost of production would range between fifty-thousand dollars and seventy-thousand dollars, and that the producing party would have to create a computer retrieval program, the court granted the plaintiff's motion to compel the defendant to produce more than thirty-million pages of e-mails and to bear the costs incurred as a result of the production.[41] The court stated that, while it seemed unfair to force a party to bear the cost of creating a retrieval program to respond to a document request, "if a party chooses an electronic storage method, the necessity for a retrieval program or method is an ordinary and foreseeable risk."[42]

However, not all courts subscribe to the notion that the existing framework for discovery in civil litigation is gospel and cannot be altered. Some courts have

---

39. Nos. 94 Civ. 897 & MDL 997, 1995 WL 360526, at *1 (N.D. Ill. June 15, 1995).

40. *Id.* at *2.

41. *Id.* at *1.

42. *Id.* at *2. In *Bills v. Kennecott Corp.*, 108 F.R.D. 459, 460 (D. Utah 1985), an age discrimination case, the plaintiffs sought production of detailed employee information stored on the defendant's computer. The defendant agreed to produce the information in either computer disk or hard copy form; however, the defendant refused to pay for the associated costs. *Id.* The court, after weighing the benefits and burdens of the discovery, declined to shift the costs onto the plaintiffs. *Id.* at 462-64. The court noted that "information stored in computers should be as freely discoverable as information not stored on computers, so parties requesting discovery should not be prejudiced thereby; and the party responding is usually in the best and most economical position to call up its own computer stored data." *Id.* at 463-64.

ordered the requesting party to bear the cost of reviewing and retrieving computerized information,[43] while other courts have recommended that the parties split the cost of copying such documents.[44] Perhaps, these courts recognize that producing hundreds of thousands of e-mails and creating retrieval programs to facilitate this process is a costly, and often an overwhelmingly arduous and burdensome, task. Nonetheless, the dichotomy that exists among the courts demonstrates that a litigant cannot predict, with certainty, his or her electronic discovery costs.

C. The Production of Deleted Computerized Information

While courts consistently have held that electronic data on computer hard drives is discoverable, to the surprise of many computer users and their lawyers, courts not only have ordered the production of retrievable deleted computerized information[45] but also have imposed sanctions for such deletions.[46] The source of the surprise is that, contrary to many computer users' beliefs, deleting a computer file or electronic communication does not erase the information from the computer. Many programs have automatic backup features that create and save a copy of the file on which the user is working.[47] However, even in the absence of a backup copy, deleted information still can be recovered. When a file is "deleted," it is marked in the computer's disk directory as "not used," thereby permitting the computer to store new files in the space where the "deleted" data exists.[48] The deleted data, while no longer appearing on the user's computer directory, remains undisturbed until the computer needs the space on the hard drive to save the

43. *In re Brand Name*, 1995 WL 360526, at *2; *see supra* note 42 and accompanying text.

44. *See, e.g.*, Sattar v. Motorola, 138 F.3d 1164, 1171 (7th Cir. 1998) (approving the trial court's recommendation that if the defendant was unable to provide the computerized information on conventional computer disks or loan the plaintiff, the requesting party, the necessary equipment to review the information, the parties each would bear half of the cost of copying).

45. *See* Simon Property Group L.P. v. mySimon, Inc., 194 F.R.D. 639, 641-42 (S.D. Ind. 2000); Easley, McCaleb & Assocs., Inc. v. Perry, No. E-2663 (Ga. Super. Ct. July 13, 1994).

46. *See* Crown Life Ins. Co. v. Craig, 995 F.2d 1376, 1383 (7th Cir. 1993); Ill. Tool Works v. Metro Mark Prods., 43 F. Supp. 2d 951, 962-63 (N.D. Ill. 1999); *In re* Prudential Ins. Co. of Am. Sales Practices Litig., 169 F.R.D. 598, 617 (D.N.J. 1997); Gates Rubber Co. v. Bando Chem. Indus., 167 F.R.D. 90, 131 (D. Colo. 1996).

47. For an in-depth discussion and explanation of how computers transform and store electronic information, see Scheindlin & Rabkin, *supra* note 34, at 333-35.

48. Scheindlin & Rabkin, *supra* note 34, at 337-38.

subsequent information.[49] Thus, unlike paper documents, which can be shredded, computer documents persist in their existence.

Similarly, deleting an e-mail message does not guarantee that the communication has been erased. To permanently delete a message in a user's e-mail directory, most e-mail programs require the user to perform a two-step deletion.[50] The user first must delete the message from his or her inbox and then must delete the message from his or her e-mail deleted items folder, recycle bin, or trash.[51] This, however, does not guarantee that the message no longer exists.[52] Most e-mail programs automatically save a copy of every message sent and received by an e-mail account.[53] Therefore, upon transmittal, one copy of the message is saved by the sender's e-mail program, another copy is saved by the recipient, and another copy is stored by the recipient's server.[54] Thus, multiple copies of an e-mail message are saved on the computers of both the sender and the recipient, even if the message is "deleted" by both.

The longevity of deleted computerized documents and e-mail has led to discovery requests seeking such information and court orders mandating their production. For example, the United States District Court for the Southern District of Indiana, in *Simon Property Group L.P. v. mySimon, Inc.*,[55] held that computer records, including records that have been deleted, are discoverable documents subject to Rule 34.[56] In granting the plaintiff's motion to compel the deleted documents, the court placed the burden and expense of obtaining the documents on the plaintiff and set forth guidelines for the task.[57] The court

---

49. The Honorable James M. Rosenbaum provided a layman's explanation of the function of the "delete" key in his article *In Defense of the DELETE Key*. *See* James M. Rosenbaum, *In Defense of the DELETE Key*, 3 GREENBAG 2D 393, 393 (2000), *available at* http://www.greenbag.org/rosenbaum_deletekey.pdf (last modified Aug. 22, 2001). Judge Rosenbaum explained:

> For those with little knowledge, and less interest, a computer's DELETE key acts somewhat like a thief who steals a card from the old library's card file. When the card was in place, the librarian could decode the library's filing system and find the book. If the card was gone, or unreadable, the book was still in the library, but it could no longer be found amidst the library's stacked shelves. In a computer, the "lost" book can be found with very little effort.

Id. at 393 n.1.

50. *See* Joan E. Feldman & Rodger I. Kohn, *The Essentials of Computer Discovery*, 564 PLI/Pat 51, 56 (1999).

51. *See id.*

52. *See id.*

53. *See id.*

54. *See id.*

55. 194 F.R.D. 639 (2000).

56. *Id.* at 640.

57. *Id.* at 641. The *Simon Property* court's guidelines were adopted from the

ordered the plaintiff to select and pay an expert to inspect and copy the hard drives of the computers in question.[58] The defendant was permitted to object to the plaintiff's selection, whereby the court would appoint the expert as an officer of the court.[59] The expert then would recover and provide, in a "reasonably convenient form, . . . all available word processing documents, electronic mail messages, powerpoint or similar presentations, spreadsheets and similar files" to the defendant's counsel.[60] The defense counsel would review the materials for privileged documents and communications, and supplement its discovery responses as necessary.[61] At the close of litigation, the expert was to destroy all records on the defendant's hard drives and confirm such destruction to the satisfaction of the defendant.[62]

Likewise, in *Easley, McCaleb & Associates, Inc. v. Perry*,[63] the Superior Court of Georgia ordered the production of all files on the defendant's hard drives, including deleted or renamed files.[64] The *Perry* court employed protocols virtually identical to those utilized by the *Simon Property Group* court.[65] The plaintiff was ordered to bear the costs of the retrieval, which included supplying the necessary equipment and software.[66] Both parties were permitted to designate a neutral computer operator or technician to assist in the copying of the defendant's hard drives.[67] The recoverable information was to be compiled and presented to the defendant to review for privileged and confidential materials; the non-privileged and non-confidential data was to be produced to the plaintiff.[68]

Notwithstanding the obvious inconvenience in producing deleted computerized information or the inevitable disruption to the functioning of a corporation or business in complying with such a request, the destruction, deletion, and failure to produce computerized information can subject an employer to sanctions. While the intentional destruction of computer data or the willful refusal to produce such discoverable records clearly may expose a litigant to sanctions,[69]

---

framework set forth in *Playboy Enters. v. Welles*, 60 F. Supp. 2d 1050, 1054-55 (S.D. Cal. 1999).

58. *Simon Property*, 194 F.R.D. at 641.

59. *Id.*

60. *Id.*

61. *Id.* at 642.

62. *Id.*

63. No. E-2663 (Ga. Super. Ct. 1994).

64. *Id.*

65. *Id.*

66. *Id.*

67. *Id.*

68. *Id.*

69. For example, in *Illinois Tool Works v. Metro Mark Products*, 43 F. Supp. 2d 951, 961 (N.D. Ill. 1999), the district court imposed sanctions on the defendant for its "purposeful effort to prevent [the] plaintiff from obtaining the information from the . . .

courts have imposed sanctions for the negligent deletion of such materials. For example, the United States District Court for the District of New Jersey imposed a $1 million sanction and ordered the reimbursement of the plaintiff's attorneys' fees due to, in part, the defendant's failure to disseminate an explicit, detailed retention policy mandating the preservation of documents.[70] Although there was no evidence of willful misconduct, the court found the defendant's "haphazard and uncoordinated approach to document retention" a sufficient basis to impose such a severe sanction.[71] Similarly, in *Gates Rubber Co. v. Bando Chemical Industries*,[72] the United States District Court for the District of Colorado ordered the reimbursement of the plaintiff's attorneys' fees and costs for the defendant's negligent deletion of some of its discoverable computer files.[73] Thus, the case law illustrates that, beyond a formalized document retention policy that provides for a specified retention period, employers should not delete or destroy computerized information—or risk being penalized.

Although courts appear to be unified in their application of Rule 34 to deleted electronic documents and communications, the Honorable James M. Rosenbaum expressed his disagreement with the state of the law concerning electronic discovery.[74] In his article, *In Defense of the DELETE Key*, Judge Rosenbaum opined "that the computer lies: it lies when it says delete."[75] According to Judge Rosenbaum, records that have been deleted by a computer user are not necessarily the "inculpatory 'second set of books.'"[76] Rather, they are often mere evidence of the user's mistakes and imperfections, documents that twenty years earlier would have been thrown in the wastebasket.[77] The problem that arises, and one

---

computer." Pursuant to a court order, the defendant was required "to preserve the integrity of all computers that are at issue here without any spoliation of any information contained therein." *Id.* at 960. Despite the defendant's repeated assertions that any computer malfunctions were entirely accidental, the court held that certain aspects of the physical condition of the computer indicated an intent to tamper with it. *Id.* at 957. The defendant was required to reimburse the plaintiff for the reasonable fees and costs of the plaintiff's computer expert, and the plaintiff's reasonable attorneys' fees and costs associated with its motion to compel and motion for sanctions. *Id.* at 962-63. In *Crown Life Insurance v. Craig*, 995 F.2d 1376, 1383 (7th Cir. 1993), the Seventh Circuit imposed sanctions upon the defendant for its failure to produce properly-requested computer data, even though the computer data was not available in hard copy form.

70. *In re* Prudential Ins. Co. of Am. Sales Practices Litig., 169 F.R.D. 598, 616-17 (D.N.J. 1997).

71. *Id.* at 615.

72. 167 F.R.D. 90 (D. Colo. 1996).

73. *Id.* at 112, 131.

74. *See generally* Rosenbaum, *supra* note 49.

75. Rosenbaum, *supra* note 49, at 396.

76. Rosenbaum, *supra* note 49, at 394.

77. Rosenbaum, *supra* note 49, at 394.

of the reasons for the proliferation of discovery requests for "deep-sea fish[ing for] snippets of deleted e-mails and deleted files," is that on the computer's hard drive, this "cyber trash" deceptively looks like more.[78] To remedy this problem, Judge Rosenbaum suggests a "cyber statute of limitations" such that, absent evidence of egregious behavior or an "objective record of systematic misconduct," courts would recognize that deleted computerized items are in fact "cyber trash."[79] Although Judge Rosenbaum did not suggest a time period for this "cyber statute of limitations" (as he noted that the length of time can be "set as arbitrarily" as any other statute of limitations), the thrust of his argument was clear—"for the law's purposes, delete would mean delete."[80] Notwithstanding that Judge Rosenbaum has yet to apply his proposal to a discovery dispute, employers should heed his warning: "[T]he computer . . . never forgets, and never forgives."[81]

III. POTENTIAL LIABILITY FOR EMPLOYERS

While e-mail technology offers speed and convenience, it also creates unique risks in the employment environment.[82] With the click of a button, one can forward an offensive or defamatory message to hundreds, perhaps thousands, of company employees, exposing employers to possible defamation, discrimination, or harassment claims.

What is it about e-mail that makes the ordinarily thoughtful person act precipitously when he or she presses the "send" button? Part of the problem is that people view e-mail much like an informal telephone conversation.[83] In many instances, statements that are written in e-mail messages would never have been written in a memorandum, correspondence, or document. These messages may be fragmented (without the use of any sentence structure), include slang terms, gossip or confidential employment information, and/or dispense with any or all of the formalities generally accepted in a corporate atmosphere. E-mail also may be forwarded or appear on a company's bulletin board for all employees to see, and it can disguise harassing conduct that otherwise would be obvious if carried out

78. Rosenbaum, *supra* note 49, at 394.

79. Rosenbaum, *supra* note 49, at 395.

80. Rosenbaum, *supra* note 49, at 395.

81. Rosenbaum, *supra* note 49, at 395.

82. *See* Mark Grossman, *Drafting an Acceptable Computer-Use Policy, How to Protect Employers from Liability Due to Employee Misuse of E-Mail and the Internet*, N.J. L.J., Sept. 6, 1999, at 33; *see also* Alan Cohen, *Keeping An Eye on Employee E-mail*, N.Y. L.J., Sept. 14, 1998, at 2; Stephen M. Foxman, *Risks from Electronic Communications—A Growing Problem*, THE METROPOLITAN CORP. COUNS., Sept. 2000, at 16.

83. *See* Grossman, *supra* note 82.

face to face.[84] For example, an employee sending a co-worker forty-nine e-mails during the course of seven business days may not alert an employer to the possible harassing conduct, but forty-nine trips to the co-worker's desk would.[85] Thus, the informality of e-mail messages and their inadvertent disclosure may expose an employer to significant liability.

A. E-mail, Discrimination, and Harassment

The widespread use of e-mail has changed the business world. Because it reduces the need for telephone calls, written memoranda, and person-to-person meetings, e-mail is an efficient and cost-saving tool for employers. E-mail has also opened the door to telecommuting, an enticing option for many employees. Yet, with all of its advantages, the emergence of e-mail in the workplace or, more specifically, the misuse of e-mail in the workplace, has exposed employers to significant liability for, among other things, discrimination and harassment. For example, in 1997, the investment banking firm Morgan Stanley & Co. was sued by two African-American employees due primarily to a racist e-mail.[86] Although the court held that one racist e-mail was insufficient evidence to support a claim for racially-hostile environment harassment, the court gave the plaintiffs leave to amend their complaint.[87] The case was later settled.[88] In *Strauss v. Microsoft Corp.*,[89] a sexual discrimination case, the plaintiff proffered e-mail messages from her supervisor containing sexually-suggestive remarks that were, in general, offensive to women.[90] The court denied the defendant's motion for summary judgment and concluded that the supervisor's behavior, including his e-mail messages, could lead a reasonable jury to conclude that the plaintiff was the victim of gender discrimination.[91] Similarly, the United States District Court for the Northern District of Illinois denied summary judgment in a sexual harassment case in which the plaintiff received e-mail messages containing sexually-explicit and suggestive images.[92] The plaintiff's supervisor was also alleged to have visited

---

84. *See* Lisa Stansky, *Changing Shifts: Does Anyone Still Work Here? As More Jobs Move from the Traditional '9 to '5, Alternative Workstyles are Forcing Redefinitions of Employment Law*, 83 A.B.A. J. 54, 58 (1997).

85. *Id.*

86. *See* Owens v. Morgan Stanley & Co., No. 96 Civ. 9747, 1997 U.S. Dist. LEXIS 10351, at *1 (S.D.N.Y. July 17, 1997).

87. *Id.* at *1-2.

88. *See* Cheryl Blackwell Bryson & Michelle Day, *Workplace Surveillance Poses Legal, Ethical Issues*, NAT'L L.J., Jan. 11, 1999, at B8.

89. 856 F. Supp. 821 (S.D.N.Y. 1994).

90. *Id.* at 822-23.

91. *Id.* at 825.

92. *See* Coniglio v. City of Berwyn, No. 99 Civ. 4475, 2000 U.S. Dist. LEXIS 9841, at *1 (N.D. Ill. June 15, 2000).

pornographic Internet web sites in the workplace and in view of other employees.[93] The court found that questions of fact existed as to whether the supervisor's misuse of the Internet and the plaintiff's receipt of harassing sexual e-mails constituted a hostile work environment.[94] Notwithstanding that some courts have held that one harassing e-mail message alone is insufficient to establish a claim of hostile environment harassment, employers and their employees should be cautious in drafting e-mail messages.[95] Employers should develop an e-mail policy that requires employees to be formal in their e-mail communications. The policy should set forth guidelines and examples of what is and what is not an acceptable e-mail message. Generally, the policy should inform employees that e-mail messages should retain the same formality as a letter sent to a corporate client. Furthermore, the policy should notify employees that their corporate or business e-mail accounts are to be used solely for business purposes and that the employer retains the right to monitor the employees' e-mails to ensure compliance with the policy. These disclosures are necessary to immunize the employer from claims that the monitoring invades the employees' right to privacy.[96] If employees are told at the outset that the employer has the right to review their e-mails for compliance purposes, the employees no longer have a reasonable expectation of privacy in the contents of their e-mail messages.[97] Finally, corporations should

---

93. *See id.*

94. *See id.*

95. *See* Curtis v. DiMaio, 46 F. Supp. 2d 206, 213 (E.D.N.Y. 1999); Owens v. Morgan Stanley & Co., No. 96 Civ. 9747, 1997 U.S. Dist. LEXIS 10351, at *7-8 (S.D.N.Y. July 17, 1997); Harley v. Michael McCoach, 928 F. Supp. 533, 540-41 (E.D. Pa. 1996).

96. *See infra* note 102.

97. Unlike public employees, employees of private corporations generally do not have a right to privacy at work. *See, e.g.*, United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000) (no expectation of privacy regarding information on an employer's computer used by an employee); Smyth v. Pillsbury Co., 914 F. Supp. 97, 101 (E.D. Pa. 1996) (no expectation of privacy in e-mail messages sent to other employees through an employer-operated e-mail system); *see also* Bohach v. Reno, 932 F. Supp. 1232, 1234-35 (D. Nev. 1996) (no expectation of privacy in telephone pager messages stored on an employer's computer). Courts that have considered the issue have focused on whether the private employee's expectation of privacy in the workplace was "reasonable." While applicable federal law provides several exceptions under which employers who provide e-mail and voicemail services to their employees via private networks may monitor those communications, the method and scope of the employer's monitoring program, as well as its demonstrated "legitimate" business need, is central to a court's determination as to whether the monitoring is permissible under certain exceptions. Additionally, while an employer may not monitor employee communications where services are provided through an outside entity, such as MCI mail, without the employee's consent, the specificity of any such consent and the implementation and maintenance of a regular monitoring program is critical to preserving the employee's consent. In California, courts

hold training sessions for their managers about their e-mail policy so that the managers effectively can communicate the policy to corporate employees and assist in its enforcement.

B. E-mail and Defamation Claims

To state a prima facie case for defamation, a statement of fact must be: (1) false and defamatory; (2) wrongly published to a third person; and (3) injurious to the plaintiff's reputation in the community.[93] Normally, a plaintiff must plead and prove special damages, i.e., specific instances of pecuniary loss due to the damage to his or her reputation. However, New York, for example, "recognizes a limited category of statements to be [defamation] *per se* which do not require pleading and proving special damages. Among these statements it is well settled that 'a writing which *tends* to disparage a person in . . . his [] profession or trade' is [defamation] *per se*."[99] Courts have been cautious, however, in finding defamatory e-mail messages actionable.[100]

Most states provide for some form of qualified immunity privilege to otherwise meritorious claims for defamation.[101] A statement is protected by the qualified privilege where it is made by someone who has an interest or duty in making it to those having a common interest in its subject matter.[102] A defendant

---

have interpreted the state constitutional right to privacy to include actions against both public and private entities. *See, e.g.*, Valley Bank of Nev. v. Super. Ct., 542 P.2d 977, 979-80 (Cal. 1975); Luck v. S. Pac. Transp. Co., 267 Cal. Rptr. 618, 627-29 (Ct. App. 1990). However, employee monitoring is subject to a "balancing test" where the employee's privacy interest must "be specifically identified and carefully compared with competing or countervailing privacy and nonprivacy interest." Hill v. Nat'l Collegiate Athletic Ass'n, 865 P.2d 633, 655 (Cal. 1994). The employee may rebut the employer's justifications for monitoring by showing that the employer could have used less intrusive methods to obtain the information sought. *Id.* at 657.

98. *See* Levin v. McPhee, 917 F. Supp. 230, 236 (S.D.N.Y. 1996).

99. Davis v. Ross, 754 F.2d 80, 82 (2d Cir. 1985) (quoting Nichols v. Item Publishers, Inc., 132 N.E.2d 860, 862 (N.Y. 1956)).

100. *See* Lian v. Sedgwick James of N.Y., Inc., 992 F. Supp. 644, 651 (S.D.N.Y. 1997) (holding that an e-mail sent by a supervisor to other departmental members stating that the plaintiff had agreed to seek other employment was not defamatory *per se*); Morrow v. II Morrow, Inc., 911 P.2d 964, 968 (Or. Ct. App. 1996) (holding that the accidental company-wide publication of a defamatory memorandum, not intended to be available on a common drive, was not adequate publication).

101. *See, e.g.*, Weldy v. Piedmont Airlines, Inc., 985 F.2d 57, 62 (2d Cir. 1993); Foster v. Churchill, 665 N.E.2d 153, 157 (N.Y. 1996); Liberman v. Gelstein, 605 N.E.2d 344, 349 (N.Y. 1992). Similarly, Texas recognizes a qualified privilege, *see* Boze v. Branstetter, 912 F.2d 801, 806 (5th Cir. 1995), as does Indiana, *see* van de Leuv v. Methodist Hosp. of Ind., Inc., 642 N.E.2d 531, 535 (Ind. Ct. App. 1994).

102. Some states that recognize a qualified privilege in communications by an

abuses its privilege where the statement is shown to be false and published: (1) with knowledge of its falsity or reckless disregard as to its truth; (2) with common malice; or (3) outside the scope of the privilege.[103]

For example, communications between managers regarding the review of an employee's job performance and the preparation of documents regarding an employee's termination are protected by a qualified privilege.[104] Similarly, an employee reference given by a former employer to a prospective employer is protected by the qualified privilege.[105] However, a qualified privilege may be overcome if the statement was made with actual malice—that is, with knowledge of its falsity and a reckless disregard for its truth.[106]

C. Postings and Bulletin Boards

Electronic company bulletin boards are potentially the riskiest form of electronic communication for employers. While they can be a cost-effective and convenient way to reach many employees with up-to-date information, ranging from work schedules to upcoming, company-sponsored employee events, electronic bulletin boards also can be a place where employees "post" defamatory or discriminatory messages about co-workers. These postings may impute liability to an employer as the bulletin board provider if a court finds that the employer is a "publisher" with editorial control. While there is no case law on

---

employer concerning an employee to persons having a corresponding interest, include but are not limited to: Texas, New York, Connecticut, Indiana, and Maine. *See Boze*, 912 F.2d at 806; *Weldy*, 985 F.2d at 62; Torosyan v. Boehringer Ingelheim Pharm. Inc., 662 A.2d 89, 104 (Conn. 1995); *van de Leuv*, 642 N.E.2d at 535; McCullough v. Visiting Nurse Serv. of S. Me., Inc., 691 A.2d 1201, 1204-05 (Me. 1997).

103. *See, e.g.*, Meloff v. N.Y. Life Ins. Co., No. 92 Civ. 7126, 1999 U.S. Dist. LEXIS 12264, at *7 (S.D.N.Y. Aug. 4, 1999) (citing *Weldy*, 985 F.2d at 62).

104. *Torosyan*, 662 A.2d at 104; *see also* RESTATEMENT (SECOND) OF TORTS §§ 593, 596 cmt. d (1977).

105. *See van de Leuv*, 642 N.E.2d at 535 (citing Chambers v. Am. Trans Air, Inc., 577 N.E.2d 612, 615 (Ind. Ct. App. 1991)); *see also Boze*, 912 F.2d at 806.

106. *See Torosyan*, 662 A.2d at 104. In *Torosyan*, for example, the appellate court affirmed the trial court's findings that:

> [the] defendant falsely attributed the plaintiff's discharge to his falsifying of company documents . . . that the plaintiff was defamed as to his business reputation . . . [that] there was sufficient publication of the allegation both among the several supervisors present at his discharge and by virtue of the written memorandum prepared at the time of his discharge and placed in his personnel file.

Id. at 102; *see* RESTATEMENT (SECOND) OF TORTS § 600 (1977); *cf. Meloff*, 1999 U.S. Dist. LEXIS 12264, at *11-12 (holding that a memorandum sent by e-mail notifying company managers, who worked with the plaintiff, that she was terminated for credit card fraud was not an abuse of qualified privilege); *van de Leuv*, 642 N.E.2d at 535.

point, one may look to court decisions and federal legislation regarding postings and online service providers ("OSPs") for possible guidance.

Much of modern case law with regard to "postings" has its roots in the New York Supreme Court's decision in *Stratton Oakmont v. Prodigy Services Co.*[107] Prior to *Stratton Oakmont*, courts held that OSPs that posted e-mail messages over their services would not be held liable for their defamatory or offensive content.[108] For example, in *Cubby v. CompuServe, Inc.*,[109] the court found for the OSP, holding that, because CompuServe had no more editorial control over a document than a public library or newsstand, it was no more liable for defamatory statements made by a distributor.[110] Similarly, in *Daniel v. Dow Jones & Co.*,[111] the court held that the Dow Jones News/Retrieval Service was a modern way for the public to obtain "up-to-the-minute-news" and, thus, was entitled to the same protection afforded a distributor.[112]

D. Publishers versus Distributors

The extent to which employers can escape liability for defamatory or harassing messages posted on their company bulletin boards by their own employees may be analogous to liability imposed on OSPs for messages posted through their services. The line between liability and non-liability for OSPs is drawn among three classifications—publishers, distributors, and common carriers.[113] An entity that exercises some degree of editorial control over the dissemination of defamatory material generally will be liable for its publication.[114] For example, a newspaper may be liable for defamation if a letter to the editor it published contains false and defamatory statements.[115] An entity that distributes but does not exercise any editorial control over defamatory material only may be liable if such entity knew or had reason to know of the defamation—such as, news vendors, books stores, and libraries.[116] However, an entity that merely acts as a passive conduit for the transmission of defamatory liability, such as a telephone

107. No. 94-31063, 1995 N.Y. Misc. LEXIS 229 (N.Y. Sup. Ct. May 24, 1995). For a discussion of *Stratton Oakmont*, see *infra* notes 118-122 and accompanying text.

108. *See* Cubby v. CompuServe, Inc., 776 F. Supp. 135, 140 (S.D.N.Y. 1991).

109. 776 F. Supp. 135 (S.D.N.Y. 1991).

110. *Id.* at 140.

111. 520 N.Y.S.2d 334 (Civ. Ct. 1987).

112. *Id.* at 340.

113. *See* Jonathan A. Friedman & Francis M. Buono, *Limiting Tort Liability for Online Third-Party Content Under Section 230 of the Communications Act*, 52 FED. COMM. L.J. 647, 651-52 (2000).

114. *See id.*

115. *See Cubby*, 776 F. Supp. at 139.

116. *Id.* at 140.

company, is not subject to defamation liability, even if such entity knew or had reason to know of the defamation.[117]

In *Stratton Oakmont*, the plaintiffs, a securities investment banking firm and its president, asserted that Prodigy was liable for allegedly defamatory statements made about the plaintiffs by an unidentified user of one of Prodigy's bulletin boards.[118] In 1994, an unidentified party, using the identification code of a Prodigy employee, posted defamatory statements on the "Money Talk" bulletin boards, stating that *Stratton Oakmont* and its president had committed criminal acts.[119] Contrary to long-standing precedent, the court found that Prodigy exercised sufficient editorial control over its computer bulletin board to render it a publisher with the same responsibilities as a newspaper.[120] The online community and Capitol Hill criticized the decision at a time when Congress was considering telecommunications reform legislation and the Communication Decency Act of 1996 ("CDA").[121] In response to the decision, Congress included a section in the CDA that effectively reversed *Stratton Oakmont*.[122] Ultimately, *Stratton Oakmont* will be remembered more for the Congressional reaction to the decision than for its reversal of precedent.

In promulgating the CDA, Congress sought to remove the disincentives to self-regulation created by the New York court's decision in *Stratton Oakmont*.[123] The CDA creates federal immunity for any state law cause of action that would hold OSPs liable for information originating from a third party.[124] Specifically,

---

117. Lunney v. Prodigy Servs. Co., No. 164, 1999 N.Y. LEXIS 3746, at *13 (N.Y. Dec. 2, 1999) (citing Anderson v. N.Y. Tel. Co., 320 N.E.2d 647 (N.Y. 1974), *cert. denied*, 529 U.S. 1098 (2000)). In *Anderson*, a minister in a religious sect sued a telephone company for failing to stop an individual from using leased telephone equipment to record messages that allegedly defamed the minister. *See Anderson*, 320 N.E.2d at 648. The New York Court of Appeals concluded that the telephone company was not the publisher and not subject to liability, even though the plaintiff had notified the phone company about the messages and the phone company refused to stop the recordings. *Id.* at 649.

118. *See* Stratton Oakmont v. Prodigy Servs. Co., No. 94-31063, 1995 N.Y. Misc. LEXIS 229, at *1 (N.Y. Sup. Ct. May 24, 1995).

119. *Id.*

120. *Id.* at *10.

121. Friedman & Buono, *supra* note 113, at 653.

122. *See* 47 U.S.C. § 230(e)(3) (Supp. V 1999) ("No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section.").

123. *See* James F. Brelsford & Nicole A. Wong, *Online Liability Issues: Defamation, Privacy and Negligent Publishing*, 564 PLI/Pat 231, 239 (1999) ("The intent of the section [509(c)(1) of the CDA] is to remove the liability 'penalty' *Stratton Oakmont* imposed on those who exercised some control over online content generated by others, including third-party statements.").

124. *See* 47 U.S.C. § 230(e)(3) (Supp. V 1999) ("No cause of action may be

§ 230(c)(1) provides: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[125] Section 230(f)(2) 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 server, including specifically a service or system that provides access to the Internet."[126] Finally, § 230(f)(3) defines "information content provider" as "any information service or any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service."[127]

E. Decisions After the CDA

Decisions since the CDA's promulgation consistently have held in favor of OSPs. In *Zeran v. America Online, Inc.*,[128] the Fourth Circuit gave an expansive reading of § 230.[129] In *Zeran*, the plaintiff claimed an unidentified third party had posted statements on a message board advertising T-shirts that glorified the Oklahoma City bombing.[130] Those interested in purchasing the T-shirts were instructed to call the plaintiff, whose home phone number was listed.[131] Plaintiff complained to America Online ("AOL"), which delayed taking the message down and refused to issue a retraction or screen for similar subsequent postings.[132] The court held that § 230 pre-empted the plaintiff's defamation and related claims, that AOL could not be treated as the "publisher" of the statements, and that even AOL's decision not to remove the posting did not render it a publisher.[133]

In *Blumenthal v. Drudge*,[134] Sidney Blumenthal, a former journalist and White House aide, and his wife, sued Matt Drudge, a publisher of an electronic publication known as the *Drudge Report*, and AOL for defamation and other claims for reporting that "top GOP operatives" believed that "Blumenthal ha[d] a spousal abuse past."[135] The plaintiff asserted that AOL, which had entered into

---

brought and no liability may be imposed under any state or local law that is inconsistent with this section.").

125. 47 U.S.C. § 230(c)(1) (Supp. V 1999).

126. 47 U.S.C. § 230(f)(2) (Supp. V 1999).

127. 47 U.S.C. § 230(f)(3) (Supp. V 1999).

128. 129 F.3d 327 (4th Cir. 1997), *cert. denied*, 524 U.S. 937 (1998).

129. *Id.* at 330-34.

130. *Id.* at 329.

131. *Id.*

132. *Id.*

133. *Id.* at 332.

134. 992 F. Supp. 44 (D.D.C. 1998).

135. *See* Brelsford & Wong, *supra* note 123, at 240 (quoting *Blumenthal*, 992 F.

a license agreement with Drudge by which it paid him a monthly royalty in exchange for the right to make the *Drudge Report* available to AOL users, jointly published the allegedly defamatory statements with Drudge and, thus, was not immune from liability pursuant to § 230.[136] The plaintiffs also alleged that AOL could be held liable on the grounds that Drudge was an employee or agent of AOL.[137] In granting AOL's summary judgment motion, the court held that the fact that AOL had the right to make changes in the *Drudge Report* was not sufficient to make it a joint publisher of the report.[138] Rather, the plaintiffs were required to present evidence that AOL had some role in creating or developing the information in the *Drudge Report* and failed to do so.[139]

In *Ben Ezra, Weinstein, & Co. v. America Online Inc.*,[140] a designer and manufacturer of corporate finance computer software sued AOL for defamation and negligence.[141] In its complaint, the plaintiff asserted that AOL defamed it on three occasions when AOL published incorrect information concerning Ben Ezra's stock price and share volume.[142] The plaintiff also claimed that AOL failed to exercise reasonable care in the manipulation, alteration, and change of the stock information.[143] The court granted summary judgment for the defendant and held that AOL acted solely as an interactive OSP,[144] and, therefore, was immune from suit under the CDA.[145] While there are no employer bulletin board cases reported under the CDA, the Act may provide guidance for future cases involving electronic bulletin boards provided by employers.

F. Electronic Bulletin Board Postings Case Not Decided Under the CDA

In the recent electronic bulletin board defamation postings case of *Blakey v. Continental Airlines, Inc.*,[146] which was not decided under the CDA, the Appellate

---

Supp. at 45).

136. *See Blumenthal*, 992 F. Supp. at 49-50.

137. *See id.* at 50.

138. *Id.*

139. *Id.* at 52-53.

140. 206 F.3d 980 (10th Cir. 2000), *cert. denied*, 531 U.S. 824 (2000).

141. *See id.* at 983.

142. *Id.*

143. *Id.*

144. *Id.* at 986. The court found that "[b]y deleting the allegedly inaccurate stock quotation information, [the d]efendant was simply engaging in the editorial functions Congress sought to protect." *Id.*

145. *Id.*; *see also* John Does v. Franco Prod., No. 99 Civ. 7785, 2000 U.S. Dist. LEXIS 8645, at *14 (N.D. Ill. June 22, 2000).

146. 730 A.2d 854 (N.J. Super. Ct. App. Div. 1999), *rev'd*, 751 A.2d 538 (2000).

Division of the New Jersey Superior Court found for the employer. In *Blakey*, Continental provided a computer bulletin board that was only accessible by its employees.[147] Defamatory remarks were published on the bulletin board (the "Forum").[148] The plaintiff claimed that she was subjected to a hostile work environment in violation of New Jersey's Law Against Discrimination ("LAD").[149] Specifically, she sought to hold Continental vicariously libel for the allegedly defamatory remarks of her co-workers.[150] The superior court found that the Forum was not a workplace under LAD and that Continental could not be held liable for the messages that appeared on the Forum because Continental had no duty to police the Internet or to control its employees' activities in a non-workplace.[151] Although this case was not decided under the CDA, it is illustrative of the treatment courts may give employer-created bulletin boards.

G. Disparate Treatment and Online Recruiting

1. E-recruiting with Resume Scanning Software

The potential for disparate treatment claims with electronic recruiting ("e-recruiting") is another risk associated with the use of technology. Emerging technology raises new issues in the area of personnel recruiting, including whether employers using software that automatically scans resumes for key words or skills, or whether employers using the Internet as their sole method of recruiting violate federal equal employment opportunity laws.[152]

The issue arose most recently in *Rivers v. Walt Disney Co.*,[153] in which four African-American employees claimed that the Walt Disney Corporation used resume scanning software to discriminate against applicants and employees unlawfully on the basis of race.[154] The complaint in *Rivers* alleged that Disney's

147. *See id.* at 856.

148. *Id.*

149. *Id.* at 856-57; *see* N.J. STAT. ANN. § 10:5-12 (West 1993 & Supp. 2001) (making it an unlawful practice for an employer to discriminate in conditions of employment).

150. *See Blakely*, 730 A.2d at 857.

151. *Id.* at 869. Further, the trial court found that Continental had no control over the Forum, that Continental did not make it a requirement for its employees to use the Forum, and that employees had to pay a service fee to CompuServe and have their own computers to access it. *Id.*

152. *See* Nadya Aswad, *Employment: Resume Scanning, Tracking Software Raises New Discrimination Issues*, DAILY LAB. REP., Mar. 17, 1998, at C-1.

153. 980 F. Supp. 1358 (C.D. Cal. 1999).

154. *Id.* at 1359. A similar suit was filed in the United States District Court for the Middle District of Florida in *Hightower v. Walt Disney World Co.*, No. 97-661-Civ-Orl-18B, 2000 U.S. Dist. LEXIS 6297 (M.D. Fla. Mar. 17, 2000).

applicant screening procedure, using a computer software program designed by Resumix, Inc., to electronically scan resumes in a database, discriminated on the basis of race.[155] The complaint further elaborated that the Resumix software electronically searched resumes in a database on the basis of "key words," identifying and activating resumes that matched and contained the selected keywords.[156] "Because of the different cultures and backgrounds, African-American applicants [were] likely to use different key words on their resumes than white applicants," the complaint went on to allege, noting that because the Resumix system is based on the primarily white culture and because "it searches for key words widely used within that culture, it discriminates against African-American applicants and employees."[157]

2. Access to Computers

In addition to disparately-selective software, the Internet has the potential to cause problems if employers who post jobs there fail to use a multifaceted search strategy including traditional means of recruiting. This may foreclose recruitment of certain racial groups, as well as older workers, who are much less conversant with web "surfing" and less likely to have access to an employer's online recruiting efforts, and it may open employers up to disparate treatment claims.

IV. TECHNOLOGY AND ITS IMPACT ON PRIVILEGED COMMUNICATIONS

The development of technology in recent years has raised new concerns regarding the protection of privileged information transmitted through e-mail systems, cellular telephones, and the Internet. These issues include whether the attorney-client privilege or work product doctrine are waived by sending confidential information via e-mail, whether an inadvertent disclosure of confidential information by e-mail waives privilege, and whether the confidences and secrets of a client are truly protected when information is relayed via modern modes of communication instead of by more traditional means.

A. The Attorney-Client Privilege and Work Product Doctrine

The attorney-client privilege applies only to communications from the client to the attorney "made for the purpose of obtaining legal advice and directed to an attorney who has been consulted for that purpose."[158] Conversely, for the

155. *See* Aswad, *supra* note 152.

156. *See* Aswad, *supra* note 152.

157. *See* Aswad, *supra* note 152 (internal citations omitted).

158. Rossi v. Blue Cross & Blue Shield, 540 N.E.2d 703, 706 (N.Y. 1989) (quoting

privilege to apply when the communications are made from attorney to client, whether or not in response to a particular request, it must be made for the purpose of facilitating the rendition of legal advice or services, in the course of a professional relationship.[159]

The attorney-client privilege applies to communications between a client and his or her attorney or a corporation and its attorney.[160] In this regard, the privilege only applies if the attorney is acting as a legal advisor.[161] Purely business communications do not fall within the privilege.[162] Thus, the risk exists that attorneys who perform multiple roles within a corporation may be found to have been acting in a strictly business capacity, rather than as a legal advisor.[163] If acting as a legal advisor, the attorney-client privilege will protect communications between the corporation's attorney and high- or low-level corporate employees.[164]

In the corporate context, the attorney-client privilege belongs to the corporation.[165] The privilege is subject to waiver by the corporation over the objections of the counsel who provided the advice because the corporation itself (but not its individual officers or employees) can choose to waive the privilege.[166] By way of example, the New York Code of Professional Responsibility mandates that a lawyer employed or retained by an organization must explain to employees and other "constituents" that he or she is the lawyer for the organization and not for any of the constituents when "it appears that the organization's interests may differ from those of the constituents with whom the lawyer is dealing."[167]

When dealing with documents, the most significant privilege is the work product doctrine. When the work product doctrine attaches to a particular document, attorneys legally may withhold the document from production in response to a discovery request.[168]

In New York, for example, the work product doctrine in civil cases is divided into two statutory provisions. First, New York Civil Practice Law and Rules Section 3101(c) provides that the "work product of an attorney" is absolutely

---

In re Bekins Record Storage Co., 465 N.E.2d 345, 348 (N.Y. 1984)).

159. *See id.*

160. *Id.*

161. *Id.* at 705.

162. *See* EDNA SELAN EPSTEIN, THE ATTORNEY-CLIENT PRIVILEGE AND THE WORK-PRODUCT DOCTRINE 95-99 (3d ed. 1997).

163. *See* Cooper-Rutter Assoc., Inc. v. Anchor Nat'l Life Ins. Co., 563 N.Y.S.2d 491, 492 (App. Div. 1990).

164. *See* Radovic v. City of New York, 642 N.Y.S.2d 1015, 1016 (Sup. Ct. 1996).

165. *See* EPSTEIN, *supra* note 162, at 166.

166. *See In re* Grand Jury Subpoenas Duces Tecum, 798 F.2d 32, 34 (2d Cir. 1986); Dooley v. Boyle, 531 N.Y.S.2d 161, 167 (Sup. Ct. 1988). *See generally* Tekni-Plex, Inc. v. Meyner & Landis, 674 N.E.2d 663 (N.Y. 1996).

167. N.Y. CODE OF PROF'L RESPONSIBILITY DR 5-109 (1998).

168. *See* EPSTEIN, *supra* note 162, at 289-91.

exempt from discovery.[169] Although Section 3101(c) does not require the attorney's protected work product be prepared in anticipation of litigation, courts have imposed this prerequisite.[170] The scope of the work product privilege has been narrowly confined by courts to those materials that are uniquely the product of a lawyer's learning and professional skills, such as materials that reflect legal research, analysis, conclusions, legal theory, or strategy.[171] A lawyer's recollections and notes of interviews with witnesses also fall within this category.[172] The work product immunity applies not only to material prepared for the litigation in progress but also to materials that were prepared in anticipation of litigation.[173]

The second work product immunity contained in Section 3101(d)(2) applies to materials prepared solely in anticipation of litigation or for trial, by or for another party, or by or for that other party's representative (including an attorney, consultant, surety, indemnitor, insurer, or agent).[174] The "solely" requirement has been interpreted narrowly. Thus, for example, investigatory reports that are motivated both by potential litigation and business considerations are not protected from discovery.[175]

Unfortunately, as in *Hickman v. Taylor*,[176] trial preparation materials are only conditionally immune from discovery. Thus, immunity can be overcome upon a showing that the party seeking discovery has a substantial need for the materials in preparation of the case and is unable, without undue hardship, to obtain the substantial equivalent of the materials by other means.[177] For example, in *Gaglia v. Wells*,[178] the defendant's statement to a liability insurer was discoverable based upon showing that the defendant could no longer recall the accident and the plaintiff suffered from amnesia.[179]

This privilege frequently will come into play when an employer's agent is conducting an internal investigation at the request and direction of the employer or the employer's counsel in anticipation of litigation. The investigative materials are conditionally immune from disclosure unless the adversary would not be able

169. N.Y. C.P.L.R. 3101(c) (McKinney 1991 & Supp. 2001); *see* Corcoran v. Peat, Marwick, Mitchell & Co., 542 N.Y.S.2d 642, 643 (App. Div. 1989).

170. *See, e.g.*, Mahoney v. Staffa, 585 N.Y.S.2d 543, 544 (App. Div. 1992); *In re* Bekins Storage Co., 460 N.Y.S.2d 684, 689-90 (Sup. Ct. 1983).

171. *See* Hoffman v. Ro-San Manor, 425 N.Y.S.2d 619, 622 (App. Div. 1980).

172. *See Corcoran*, 542 N.Y.S.2d at 643-44.

173. *See* Beasock v. Dioguardi Enters., Inc., 499 N.Y.S.2d 560, 560 (App. Div. 1986).

174. N.Y. C.P.L.R. 3101(d)(2) (McKinney 1991 & Supp. 2001).

175. *See* Carlo v. Queens Transit Corp., 428 N.Y.S.2d 298, 299 (App. Div. 1980).

176. 329 U.S. 495 (1947).

177. *See* Barton v. Diesel Constr. Co., 365 N.Y.S.2d 197, 198 (App. Div. 1975).

178. 490 N.Y.S.2d 829 (App. Div. 1985).

179. *Id.* at 830.

to obtain the equivalent of the materials by other means (for example, in a situation where a witness is no longer available to testify).[180]

B. E-mail, Cellular Telephones, and the Internet, and Their Impact on Privileged Communications

1. Three Approaches Utilized by the Courts Regarding New Technology and Privileged Communications

The primary concern with advancing technology and its effect on privileged communications is whether the use of e-mail, cellular telephones, and the transmission of confidential materials over the Internet will increase the likelihood that a court will find that the attorney-client privilege or work product doctrine has been waived, particularly in situations of inadvertent disclosure.[181] Courts have addressed the "accidental" waiver issue with burgeoning technology by utilizing one of three already-established approaches. These approaches include: (1) the strict liability test; (2) the intent test; and (3) the case-specific test.[182] Although the application of these tests to questions of privilege is not new, the application of the tests to modern modes of communication is novel. As a result, lawyers should take precautionary measures whenever communicating with a client via e-mail, cellular telephones, or the Internet. In order to determine what precautions a lawyer should take, a brief synopsis of the three applicable tests is necessary.

First, the strict liability test holds that disclosure of any kind, including inadvertent disclosure, constitutes a waiver of the attorney-client privilege and work product doctrine.[183] The theory supporting this analysis is that once information is disclosed, it forever will remain disclosed. Therefore, any prior privilege to keep such information confidential is destroyed.[184]

The second approach is the intent test. Under this test, confidential communications may be waived only if the disclosing party had the specific intent

---

180. *See id.*; *Barton*, 365 N.Y.S.2d at 198.

181. *See generally* Carter v. Gibbs, 909 F.2d 1452, 1458 (Fed. Cir.), *cert. denied sub nom.* Carter v. Goldberg, 498 U.S. 811 (1990); Fidelity & Deposit Co. of Md. v. McCulloch, 168 F.R.D. 516, 521 n.4 (E.D. Pa. 1996); Hartford Fire Ins. Co. v. Garvey, 109 F.R.D. 323, 328 (N.D. Cal. 1985).

182. *See* 8 JOHN H. WIGMORE, EVIDENCE IN TRIALS AT COMMON LAW § 2290 (J.T. McNaughton, rev. 1961); Bank Brussels Lambert v. Credit Lyonnais, 160 F.R.D. 437, 442 (S.D.N.Y. 1995); Fed. Deposit Ins. Corp. v. Marine Midland Realty Credit Corp., 138 F.R.D. 479, 482 (E.D. Va. 1991); Helman v. Murray's Steaks, Inc., 728 F. Supp. 1099, 1104 (D. Del. 1990); Hartford Fire Ins. Co. v. Garvey, 109 F.R.D. 323 (N.D. Cal. 1985); *see also infra* notes 183-89 and accompanying text.

183. *See* 8 WIGMORE, *supra* note 182, § 2290.

184. *See* United States v. Kelsey-Hayes Wheel Co., 15 F.R.D. 461, 465 (E.D. Mich. 1954).

to waive the privilege.[185] Courts utilizing this approach opine that waiver of the attorney-client privilege or work product doctrine requires some degree of intent. Absent such intent, waiver is not possible.[186]

The last approach, which is utilized by a majority of the courts, is the case-specific test.[187] This test focuses on the totality of the circumstances. Many factors are considered under this test, including: "(1) the reasonableness of precautions taken to prevent disclosure; (2) the amount of time taken to remedy the error; (3) the scope of discovery; (4) the extent of disclosure; and (5) the overriding issue of fairness."[188] Therefore, the measure of reasonable precautions taken by an attorney to keep the secrets of his or her client determines whether any kind of disclosure constitutes a waiver of the attorney-client privilege or of the work product doctrine.[189]

2. E-mail

E-mail is an electronic system that allows immediate and efficient communication between individuals. In today's legal environment, attorneys often transmit confidential client information over the Internet via unencrypted e-mail.[190] The transmission of such information raises evidentiary issues of privilege and potential ethical concerns.

a. Evidentiary Rules Regarding E-mail and Privileged Communications

State laws regarding new modes of communication and their effect on the law of privilege are slowly developing. For example, on July 7, 1998, the New York Civil Practice Law and Rules was amended to clarify New York's law regarding the electronic communication of privileged information.[191] Section 4548 was added, which provides:

185. *See Helman*, 728 F. Supp. at 1104.

186. *See* Mendenhall v. Barber-Greene Co., 531 F. Supp. 951, 954 (N.D. Ill. 1982).

187. *See generally Hartford Fire Ins. Co.*, 109 F.R.D. at 329 ("Rather, the modern trend seems to be towards a case by case determination of waiver based on a consideration of all the circumstances. The majority of cases do hold, or take for granted, that inadvertent disclosure of privileged documents may waive the privilege.").

188. Alldread v. City of Grenada, 988 F.2d 1425, 1433 (5th Cir. 1993).

189. When applying the case-specific test, some courts will consider Fourth Amendment principles regarding a person's reasonable expectation of privacy in order to determine whether inadvertent disclosure constitutes a waiver. *See* Katz v. United States, 389 U.S. 347, 350 (1967).

190. Encryption is a security measure that jumbles an e-mail message, thereby rendering it unreadable in order to protect its contents from an unintended recipient.

191. *See* N.Y. C.P.L.R. 4548 (McKinney Supp. 2001).

> No communication privileged under this article shall lose its privileged character for the sole reason that it is communicated by electronic means or because persons necessary for the delivery or facilitation of such electronic communication may have access to the content of the communication.[192]

New York was one of the first states to pass an electronic communications law.[193] The CPLR Committee of the New York State Bar Association proposed this new statute, arguing "e-mail communications have become effective means of communications which should be encouraged."[194] This legislative finding essentially provides assurance to attorneys that e-mail transmissions of privileged information have a reasonable expectation of privacy. This, in turn, supports the contention that e-mail transmissions are protected by the attorney-client privilege. Several state judicial opinions also have supported this contention, stating that e-mail communications should be analogized to and treated the same as other more traditional means of communication.[195] Nevertheless, attorneys should proceed cautiously when sending privileged information via e-mail because ethical considerations remain unsettled. The New York State Bar Association's Supporting Statement to the new section was clear in stating:

> [Section 4548 does not] deal with the duty of a professional to preserve clients' secrets. While a communication over E-mail may be sufficiently confidential that it does not waive the evidentiary privilege that attaches to it, the obligation of a professional to keep confidences may require that certain highly confidential matters not be communicated in this form, even though it would be privileged.[196]

---

192. N.Y. C.P.L.R. 4548 (McKinney Supp. 2001).

193. California also passed an electronic communications law in 1994. *See* CAL. EVID. CODE § 952 (West 1995). Its law provides: "[a] communication between a client and his or her lawyer is not deemed lacking in confidentiality solely because the communication is transmitted by facsimile, cellular telephone, or other electronic means between the client and his or her lawyer." CAL. EVID. CODE § 952 (West 1995).

194. N.Y. St. B. Ass'n, CPLR Comm., *Privileged E-Mail Proposal: CPLR § 4547 supporting statement, available at* http://www.nysba.org/committees/cplr/library/4547.html (last visited Nov. 14, 2001).

195. *See, e.g.*, McCook Metals L.L.C. v. Alcoa, Inc., 192 F.R.D. 242, 255 (N.D. Ill. 2000); Playboy Enters., Inc. v. Welles, 60 F. Supp. 2d 1050, 1054 (S.D. Cal. 1999).

196. N.Y. St. B. Ass'n, CPLR Comm., *Privileged E-Mail Proposal: CPLR § 4547 supporting statement, available at* http://www.nysba.org/committees/cplr/library/4547.html (last visited Nov. 14, 2001).

b. Ethical Rules Regarding E-mail and Privileged Communications

Although information transmitted via e-mail retains its privileged character, attorneys must ensure that they are abiding by the ethical rules of professional conduct. The American Bar Association ("ABA") and several state ethics committees have addressed this issue in formal written opinions.

The transmission of unencrypted confidential information may raise ethical concerns because the ABA Model Rule of Professional Conduct 1.6(a) prohibits an attorney from revealing confidential client information absent the client's consent after consultation and imposes a duty on a lawyer to take reasonable steps under the circumstances to protect such information against unauthorized disclosure.[197]

On March 10, 1999, the ABA Standing Committee on Ethics and Professional Responsibility allayed the concerns of many attorneys and stated that an attorney may transmit information relating to the representation of a client by unencrypted e-mail sent over the Internet without violating his or her ethical obligations.[198] The Committee based its opinion on the fact that Model Rule 1.6 only requires a lawyer to choose a means of communication in which the lawyer has a reasonable expectation of privacy.[199] An absolute expectation of privacy is not required. The Committee found that unencrypted e-mail communications sent over the Internet pose no greater risk of interception or disclosure than other modes of communication commonly relied upon as having a reasonable expectation of privacy.[200]

The Committee did note, however, that, if the confidential client information being transmitted is so highly sensitive that extraordinary protective measures are warranted, the lawyer should consult with the client as to whether another mode of delivery is warranted and should follow the client's instruction as to the mode of transmission.[201] In such a highly sensitive situation, an attorney probably

197. *See* MODEL RULES OF PROF'L CONDUCT R. 1.6(a) (1980). *See generally* Iowa Sup. Ct. Bd. of Prof'l Ethics and Conduct, Op. 96-01 (1996) (holding that "sensitive material" sent across the Internet via e-mail by an attorney must be encrypted, and, if it cannot be encrypted, the attorney must inform the client of the risks the e-mail communication poses on the expectation of privacy); S.C. St. B. Ass'n Ethics Advisory Comm., Advisory Op. 94-27 (1995) (opining that there is little expectation of privacy when transmitting e-mail over the Internet).

198. *See* ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 99-413 (1999).

199. *See* MODEL RULES OF PROF'L CONDUCT R. 1.6(a) (1980).

200. *See* ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 99-413 (1999); *see also* United States v. Charbonneau, 979 F. Supp. 1177 (S.D. Ohio 1997) (holding that expectation of privacy for e-mail is analyzed in the same manner as a letter sent via U.S. mail).

201. *See* ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 99-413

should not use e-mail as a means of communicating with his or her client without utilizing additional safeguards.

In New York, DR 4-101 of the Code of Professional Responsibility provides, in relevant part, that "a lawyer shall not knowingly . . . [r]eveal a confidence or secret of a client."[202] The CPLR Committee of the New York State Bar Association, commenting on this Section of the Code of Professional Responsibility, cautioned:

> [T]he obligation of a professional to keep confidences may require that certain highly confidential matters not be communicated [by e-mail], even though it would be privileged. A confession of a crime, the communication of a sensitive trade secret or similar information ordinarily should be communicated in a method designed to ensure that no third party has access to the information under any circumstances.[203]

Therefore, the mode of communication chosen by an attorney to transmit information to his or her client, or a third party, whether it be through electronic, written, or oral means, must be appropriate under the circumstances to protect the confidences and secrets of the client.

Most states that have been presented with this issue have found that e-mail communications with a client are not a *per se* violation of the rules of ethics.[204] For example, the Illinois State Bar Association, in an advisory opinion, found that an attorney does not violate its ethical rules by communicating with his or her client via e-mail because there is a reasonable expectation of privacy, which is no less reasonable than the expectation of privacy for telephone calls.[205] Moreover, the interception of e-mail through fraudulent means or for fraudulent purposes has no effect on the privileged character of an e-mail transmission because such conduct is illegal under the Electronic Communications Privacy Act of 1986 ("ECPA").[206]

The District of Columbia Bar Association also addressed this issue and found that confidential e-mail communications do not violate its ethical rules of

---

(1999).

202. N.Y. CODE OF PROF'L RESPONSIBILITY DR 4-101 (2000).

203. N.Y. St. B. Ass'n, CPLR Comm., *Privileged E-Mail Proposal: CPLR § 4547 supporting statement, available at* http://www.nysba.org/committees/cplr/library/4547.html (last visited Nov. 14, 2001).

204. *See infra* notes 205-11.

205. *See* Ill. St. B. Ass'n, Op. 96-10 (1997).

206. *See id.*; *see also* ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 99-413 (1999) (finding that "[i]t is not . . . reasonable to require that a mode of communicating information must be avoided simply because interception is technologically possible, especially when unauthorized interception or dissemination of the information is a violation of law").

conduct.[207] It noted, however, that, in instances where communications require a "higher level of security," the use of encrypted e-mail transmissions should be considered and will be adequate to protect confidentiality.[208]

Similar opinions have been expressed by the Vermont Bar Association,[209] the Alaska Bar Association,[210] and the Pennsylvania Bar Association.[211] The majority of state bar associations agree, however, that under some circumstances, unencrypted e-mail communications may violate a lawyer's ethical obligations to his or her client.

3. Cellular Telephones

Although the use of cellular telephones has facilitated communications between attorney and client, it also has created new legal risks concerning the interception of such communications. Congress reacted to this new technological development by passing ECPA in 1996. ECPA provides: "no otherwise privileged wire, oral or electronic communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character."[212]

Despite ECPA's enactment, state ethics committees, as well as the ABA, have issued their own opinions regarding the dissemination of confidential communications over cellular telephones. In New York, the Association of the Bar of the City of New York wrote a formal opinion, wherein it stated: "[a] lawyer should exercise caution when engaging in conversations containing or concerning client confidences or secrets by cellular or cordless telephones or other communication devices readily capable of interception, and should consider taking steps sufficient to ensure the security of such conversations."[213] Several other states have taken a similar position.[214]

Furthermore, the ABA Committee on Ethics and Professional Responsibility expressed its concerns about the use of cellular telephones to transmit confidential information to a client.[215] Although the Committee did not resolve the issue, it

207. *See* D.C. B. Ass'n, Op. 281 (1998).

208. *See id.*

209. Vt. B. Ass'n, Op. 97-5 (1997).

210. Alaska B. Ass'n Ethics Comm., Op. 98-2 (1998).

211. Pa. B. Ass'n Comm. on Legal Ethics and Prof'l Responsibility, Op. 97-130 (1997).

212. *See* 18 U.S.C. § 2517(4) (1994).

213. Ass'n of the B. of the City of N.Y., Comm. on Prof'l and Judicial Ethics, Formal Op. 1994-11 (1994).

214. *See* Mass. B. Ass'n Ethics Comm., Op. 94-5 (1994); N.H. B. Ass'n, Advisory Op. 1991-902/6 (1992).

215. *See* ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 99-413 (1999).

found that communications transmitted over cellular telephones may be less secure than communications transmitted over "land-line" telephones.[216] Therefore, attorneys should be careful not to reveal highly sensitive information over cellular telephones.

4. Interception of E-mail and Cellular Telephones

E-mail and cellular telephone conversations illegally intercepted do not lose their privileged status.[217] Under ECPA, privileged communications, including electronic communications, retain their privileged character in the event they are intercepted in violation of the law.[218] Many states, such as New York, have followed the federal government's lead and enacted state legislation to protect the privileged character of communications sent via e-mail.[219]

---

216. *See id.*

217. Employee communications may be monitored under the "business related" exceptions to the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510-20 (amended by the Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-22 (1994 & Supp. V 1999)), and are, therefore, subject to disclosure. However, courts uniformly have found that employers may not surreptitiously monitor their employees' personal communications. *See* Epps v. St. Mary's Hosp. of Athens, Inc., 802 F.2d 412, 417 (11th Cir. 1986) (employee telephone calls that included disparaging comments about their supervisors and were placed from company telephones during working hours were "business related" because the employer has legal interest in the content of telephone calls with the "potential [of] contaminat[ing] the work environment"); Briggs v. Am. Air Filter Co., 630 F.2d 414, 415-16 (5th Cir. 1980) (an employer's monitoring of an employee's telephone conversations via an extension telephone located in another office was in the "ordinary course of business," where the employer "highly suspected" that the employee was disclosing confidential information to a competitor); Arias v. Mut. Cent. Alarm Servs., Inc., 182 F.R.D. 407 (S.D.N.Y. 1998) (twenty-four-hour recording of all calls to and from a security company were found to be "business related" because such companies are "repositories of extremely sensitive security information, including information that could facilitate access to their customers' premises" by criminals, as well as police and fire departments); Tiberino v. Spokane County, 13 P.3d 1104, 1108-09 (Wash. Ct. App. 2000) (while the number of a public employee's personal e-mails was discoverable, the content of personal e-mails was not subject to disclosure). *But see* Watkins v. L.M. Berry & Co., 704 F.2d 577, 583 (11th Cir. 1983) (an employer's monitoring of an employee's personal telephone calls under its policy as part of its telephone sales training program violated the ECPA where the employer failed to show compelling business need).

218. *See* 18 U.S.C. §§ 2510-22 (1994 & Supp. V 1999).

219. *See* N.Y. C.P.L.R. 4548 (McKinney Supp. 2001).

5. Internet and Intranet Use

Generally, computer electronic communications networks fall into one of two categories—Internet systems and *Intranet* systems. A basic understanding of the differences between the two is germane to understanding the legal responsibilities placed upon employers regarding the management of its communications.[220]

An Intranet is a network that, although based on Internet protocols, is privately owned by a company and is self-contained, accessible solely by the company's employees or others with authorization.[221] Today, nearly ninety percent of all companies use Intranets.[222] Unlike Internet systems that utilize public telephone lines, Intranet users are directly connected, and the messages are not transmitted over public telephone lines.[223] While an Intranet's web site and e-mail system appear and function in the same manner as they would on the Internet, a closed Intranet network maintains a barrier or "firewall" that prevents unauthorized access.[224] Firewalls are systems, implemented through both computer hardware and software, designed to prevent unauthorized access from the Internet into the private network.[225] All messages entering or leaving the Intranet must pass through the firewall, which enables the messages to be examined and blocked if they fail to meet specific security criteria.[226] The use of a firewall is essential for employer Intranet systems because such use likely will be viewed by courts as a reasonable precaution taken by an employer to maintain its expectation of privacy, and, therefore, to retain the protections afforded by the attorney-client privilege and work product doctrine.

Although an Intranet can be operated as a closed network, most companies link their private Intranets to the public Internet.[227] Ordinarily, companies facilitate that connection through an agreement with an Internet service provider ("ISP"), under which the company's employees access the Internet through

---

220. For a more in-depth description of the history of the Internet and modes of access, see, for example, *American Civil Liberties Union v. Reno*, 929 F. Supp. 824, 830-40 (E.D. Pa. 1996).

221. Jared D. Beeson, *Cyberprivacy on the Corporate Intranet: Does the Law Allow Private-Sector Employers to Read Their Employees' E-mail?*, 20 U. HAW. L. REV. 165, 170 (1998).

222. Caitlin Garvey, Comment, *The New Corporate Dilemma: Avoiding Liability in the Age of Internet Technology*, 25 U. DAYTON L. REV. 133, 136 (1999).

223. Beeson, *supra* note 221, at 170.

224. Webopedia, *Intranet*, *at* http://www.webopedia.com/term/i/intranet.html (last visited Nov. 15, 2001).

225. Webopedia, *Firewall*, *at* http://www.webopedia.com/term/f/firewall.html (last visited Nov. 15, 2001).

226. *Id.*

227. Garvey, *supra* note 222, at 136.

telephone lines for which the company pays a fee.[228] Generally, ISPs operate Internet servers and also provide services such as e-mail, web-page hosting, or usernet newsgroups.[229] Currently, under relevant statutory law, what constitutes an ISP remains unclear.[230] For instance, under the Digital Millennium Copyright Act, "service provider" is defined as "an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received."[231] In general, the ISP label includes all organizations that provide Internet-related services.[232] The more companies that link their private Intranets to the Internet, the more they meet the functional definition of an ISP with the attendant immunity from liability. Thus, companies with direct links to the Internet appear to meet the functional definition of an ISP.

V. CONCLUSION

While the business and legal communities have welcomed the freedom and rapid accessibility of information that modern technology has made possible with open arms, today's new communications technologies have created pitfalls, and have and will continue to raise liability issues that must be carefully considered by employers and their counsel in day-to-day communications, litigation, and employee relations for years to come. Most, if not all, of the pitfalls certainly can be avoided by careful legal document handling, clear and consistent employee monitoring, and carefully drafted employee use policies.

228. Garvey, *supra* note 222, at 140.

229. Garvey, *supra* note 222, at 137. These providers, however, are occassionallly distinguished from telecommunications providers such as AT&T and UUNET, which are more commonly known as "Internet Backbone Providers."

230. Garvey, *supra* note 222, at 138-39.

231. 17 U.S.C. § 512(k)(1)(A) (Supp. V 1999).

232. Garvey, *supra* note 222, at 137.