COMMENT

SAFETY IN NUMBERS: REVISITING THE RISKS TO CLIENT CONFIDENCES AND ATTORNEY-CLIENT PRIVILEGE POSED BY INTERNET ELECTRONIC MAIL

By Joshua M. Masur[†]

ABSTRACT

Courts have not yet considered the application of the attorney-client privilege to electronic mail transmitted over the Internet. Despite the absence of a definitive ruling on the issue, legal commentators and ethics committees have presented opinions that tend to conclude that the privilege applies to electronic mail. This Comment addresses the possibility that these legal opinions are based on misconceptions about the underlying technology and security of Internet transmitted electronic mail. This Comment critically evaluates legal opinions regarding the relationship of the privilege to electronic mail by explaining the pertinent technology and security issues that attorneys should be aware of when discussing sensitive information with their clients over Internet transmitted electronic mail. Given the relative ease with which unencrypted electronic mail can be intercepted by third parties, encryption presents one cautionary measure that can be taken by attorneys seeking to ensure that communications with their clients remain privileged.

---

† J.D. 1999, Columbia Law School; A.B. 1990, Columbia College of Columbia University. Prior to attending law school, Mr. Masur worked in the computer and networking industries for eight years, including stints as director of management information services for a nonprofit law firm, director of consulting services for a computer consulting company, and computer technology manager for an international advertising agency. This article represents the views of the author only, and is not to be attributed to any client or employer of the author.

The author wishes to thank the editorial staff of the Berkeley Technology Law Journal for their assistance and dedication; Richard Ziegler, for having suggested and guided his research into this topic; Michael Geist, for early editorial advice and input; Lance Liebman, for requesting that he teach relevant portions of this material in his course on telecommunications law; those unfortunate members of Columbia Law School's class of 2000 whom he forced to argue these issues as first-year students in Moot Court; and Shelly K. Masur and Julia Astrid Masur, for their love, understanding, and support.

This Comment was the first-place winner of the 1999 *Berkeley Technology Law Journal* Comment Competition.

TABLE OF CONTENTS

I. INTRODUCTION

Throughout much of the 1990s, one of the livelier questions in legal ethics was whether unencrypted electronic mail sent over the Internet could sustain the attorney-client privilege. If any case law issued, it went unnoticed, but state ethics committees and law journal pundits issued

competing analyses of the potential weaknesses of e-mail. As the decade wore on, however, skeptical voices were drowned out by the chorus of well-meaning commentators who insisted that e-mail was just like the telephone, fax, or postal mail, and nothing like a cellular phone, radio broadcast, or crowded public place. Then, in the spring of 1999, the American Bar Association Standing Committee on Ethics and Professional Responsibility joined the fray with a voice of authority:

> 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 (1998) 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.[1]

The Committee hedged that its opinion was "based upon current technology and law *as we are informed of it*,"[2] but the message was clear: lawyers could use e-mail to communicate with clients in much the same way as they would a telephone or fax.

There are two problems with this opinion. First, the Committee, like many other contemporary commentators, betrayed the long-standing mandate that the attorney-client privilege ought to be treated as the exception to the general rule that all testimony should be admitted as evidence before a court.[3] While some intellectual defense for this conclusion can be found in the courts' recent tendency to apply the privilege with great frequency rather than great scrutiny, one should be cautious about thinking of this judicial change in applying the privilege as sufficient ground for the ABA opinion. Judicial goals often differ from the goals for organizations like the ABA.

The second problem is thornier. The Committee was wise to warn that its opinion depended on its understanding of the technology at issue. It would have been wiser still to base its understanding on the appropriate technological research. Instead, every technical pronouncement in the

---

1. ABA Comm. on Ethics and Professional Responsibility, Formal Op. 99-413 (1999) (on protecting the confidentiality of unencrypted e-mail) *available at* <http://www.abanet.org/cpr/fo99-413.htm> [hereinafter ABA Op.].

2. *Id.* (emphasis added).

3. *See In re* Horowitz, 482 F.2d 72, 81 (2d Cir.), *cert. denied*, 414 U.S. 867 (1973) ("[Privilege] is to be strictly confined within the narrowest possible limits consistent with the logic of its principle.").

opinion is cited not to a source with some technical pedigree, but to a law journal article.

The most stunning example of the Committee's attempt to draw a conclusion based on a misunderstanding of the technology is the following uncited assertion: "Because the specific route taken by each e-mail message through the labyrinth of phone lines and ISPs is *random*, it would be very difficult consistently to intercept more than a segment of a message by the same author."[4] While empirical research conclusively demonstrates this proposition as erroneous,[5] a small degree of common sense reveals its absurdity: if "the specific route taken by each e-mail message ... is random," how on earth does the message reach its intended recipient? To use a real-world analogy, how many of us would respond to a request for directions to our homes by saying, "just drive—you'll get there eventually"? Routing is the foundation of the Internet, without which there is no internetwork communication, only individual networks. This is the ABA's most striking misconception of the way in which the Internet works; that it exists in a document that purports to establish rules for Internet use is profoundly disturbing, made worse by the implicit contention that it is common knowledge, undeserving of citation.

The sad fact is that by the time the ABA weighed in on privilege issues and electronic mail, the discussion of privilege for electronic mail was little more than an incestuous game of telephone. Technical concepts like "dynamic routing," where the Internet's traffic cops direct messages along what they believe to be the most efficient route, had become perverted into the mythical "random routing"—mythical because it betrays more about its proponents' desires than about objective truth. The ABA opinion thus stands as the stunning apotheosis of a debate that had long ago lost its objective moorings. The members of the debate quoted one another, secure in the belief that they had ascertained the truth. Unfortunately, by convincing themselves, they may well have convinced enough others that their ungrounded beliefs will take on the force of law.

This Comment considers the possibility that some court will find that unencrypted electronic mail sent over the Internet is insufficiently confidential to maintain the attorney-client privilege over its contents. Part II discusses the law of attorney-client privilege, focusing on the requirements of contemporaneous confidentiality and subsequent non-waiver. Part III provides an introduction to the benefits and dangers of e-mail and discusses encryption and its limitations. Part IV analyzes in detail the security

4. ABA Op., *supra* note 1 (emphasis added).
5. *See infra* Part IV.C.1.

issues surrounding unencrypted electronic mail sent over the Internet. Finally, Part V proposes protective measures for attorneys who wish to minimize incursions into their private communications with their clients, but who do not wish to forego the benefits available from the use of electronic mail in such communications.

II. THE ATTORNEY-CLIENT PRIVILEGE

The classic formulation of the attorney-client privilege can be found in Wigmore. The privilege applies:

> (1) Where legal advice of any kind is sought (2) from a professional legal advisor in his capacity as such, (3) the communications relating to that purpose, (4) made in confidence (5) by the client, (6) are at his instance permanently protected (7) from disclosure by himself or by the legal advisor, (8) except the protection be waived.[6]

A simplified version of this test is proposed by the Restatement (Third) of the Law Governing Lawyers, which provides that "the attorney-client privilege may be invoked ... with respect to: (1) a communication (2) made between privileged persons (3) in confidence (4) for the purpose of obtaining or providing legal assistance for the client."[7] Both of these definitions apply best when the client is a natural person, rather than an artificial entity like a corporation, the subjective intent of which is difficult to gauge. Thus, application of the privilege to corporate entities is controlled by the test announced by the Supreme Court in *Upjohn Co. v. United States*.[8] *Upjohn* provides an eight-prong test similar to that of Wigmore. Under *Upjohn*, the attorney-client privilege protects:

> [1] communications ... by ... employees [2] to counsel ... acting as such, [3] at the direction of corporate superiors [4] in order to secure legal advice from counsel ... [5] concern[ing] matters within the scope of the employees' corporate duties ... [6] [where] employees themselves were sufficiently aware that they were being questioned in order that the corporation could obtain legal advice ... [7] communications were considered "highly

6. 8 JOHN HENRY WIGMORE, EVIDENCE § 2292, at 554 (McNaughton rev. 1961) (emphasis omitted).

7. RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS § 118 (Proposed Final Draft No. 1, 1996) [hereinafter RESTATEMENT].

8. 449 U.S. 383 (1980).

> confidential" when made ... and [8] have been kept confidential by the company.[9]

These requirements act to limit privilege to those communications where protection is judged necessary. "While the professional obligation to keep client information secret is a hallmark of professional practice, confidentiality can also be exploited to violate the law. The rules of confidentiality therefore provide exceptions to guard against abuse."[10]

The applicability of attorney-client privilege to electronic mail communications hinges on the seventh and eighth factors of the *Upjohn* test, and the corresponding fourth and eighth Wigmore factors—that the communication be intended to be confidential and that the privilege not be waived.[11] For the attorney-client privilege to attach, a party must have contemporaneously intended to keep confidential any communication over which attorney-client privilege is asserted. That confidentiality must not have been waived, either inadvertently or intentionally. Furthermore, because the privilege is an exception to the rule that all testimony should be admitted as evidence before the court, the privilege "ought to be strictly confined within the narrowest possible limits consistent with the logic of its principle."[12] Thus, application of the privilege to unencrypted electronic mail cannot be presumed without meaningful inquiry.

A. State of the Law: Lack of Controlling Precedent

As one commentator stated, "no one yet knows whether or not courts will determine that sending an e-mail message over the Internet waives the attorney-client privilege."[13] This lack of predictability is amplified because communication over the Internet is fundamentally different from other forms of communication, as the Supreme Court noted in *Reno v. American Civil Liberties Union*.[14] Thus, existing privilege case law may not map efficiently or effectively onto e-mail.

Failure to use encryption to protect electronic mail communications may, in and of itself, indicate lack of intent or actual failure to maintain

---

9. *Id.* at 394-95.

10. RESTATEMENT, *supra* note 7 at introductory note to chapter 5.

11. *See, e.g.*, Jonathan Rose, Note & Comment, *E-mail Security Risks: Taking Hacks at the Attorney-client Privilege*, 23 RUTGERS COMPUTER & TECH. L.J. 179, 182 (1997) ("In applying the attorney-client privilege to e-mail, ... the most crucial elements to consider are the requirements that the communications be confidential and that the privilege has not been waived.").

12. *See In re* Horowitz, 482 F.2d 72, 81 (2d Cir.), *cert. denied*, 414 U.S. 867 (1973).

13. Todd H. Flaming, *Internet E-mail and the Attorney-Client Privilege*, 85 ILL. B.J. 183, 183 (1997).

14. 117 S. Ct. 2329 (1997).

confidentiality. This is, however, a matter of unsettled law. No reported case addresses the effect of e-mail communication on the privilege.[15] The closest that reported federal decisions have come to this issue is reviewing electronic mail sent over in-house or private networks, without considering issues unique to Internet-based communication.[16] Some state ethics boards have found more limited protection for unencrypted electronic mail sent via the Internet. Iowa and South Carolina require express consent by the client to use of unencrypted e-mail, while Illinois treats electronic mail as an "ordinary telephone call."[17] However, ethics panels in other states and the American Bar Association consider unencrypted electronic mail to be fully entitled to privileged treatment.

1. Statutory Approaches to the Privilege and the Internet

Ethics boards and legislatures have disagreed as to whether and how the attorney-client privilege should apply to unencrypted e-mail communications over the Internet.[18] This problem is compounded by the nature of the Internet itself. "Since the Internet defies state boundaries, it is difficult to know how e-mail that is not purely local should be handled. Worse, the confusion seems to surround not only the technology, which is relatively new, but the attorney-client privilege itself, which is as old as the profession."[19]

Several states have provisions under which privilege is maintained despite interception; most are analogous to the federal Electronic Communications Privacy Act ("ECPA").[20] New York's recently-enacted Civil Practice Law and Rules section 4548, adopted in 1997, is fairly typical:

> Privileged Communications; Electronic Communication Thereof. 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

15. *See* Julienne W. Bramesco, *Employee Privacy: Avoiding Liability in the Electronic Age*, 562 PLI/LIT 515, 527 (1997).

16. *See, e.g.*, United States v. Keystone Sanitation Co., 903 F. Supp. 803, 808 (M.D. Penn. 1995); Int'l Marine Carriers v. United States, No. 95 Civ. 10670, 1997 WL 160371 (S.D.N.Y. Apr. 4, 1997); Heidelberg Harris v. Mitsubishi Heavy Indus., No. 95 C 0673, 1996 WL 732522 (N.D. Ill. Dec. 18, 1996).

17. *See* Wendy R. Leibowitz, *Communication in the E-mail Era: Deciphering the Risks and Fears*, NAT'L L.J., Aug. 4, 1997, at B9. *See also infra* Part V.

18. *See* Leibowitz, *supra* note 17.

19. *See id.*

20. 18 U.S.C. §§ 2510-2520 (1982) (amended 1994).

> delivery or facilitation of such electronic communication may have access to the content of the communication.[21]

However, at least one pre-enactment commentator noted that this section "does not address unauthorized access by snoopers who have nothing to do with the transmission of an electronic message."[22] Furthermore, reliance on illegality of interception may be misplaced, especially given the wording of the law, which does not apply the privilege for communications that would otherwise lack it.[23]

2. *Ethics Committee Opinions on E-mail Privilege Issues*

Ethics committee opinions on the role of encryption in privilege issues varied during the 1990s. In 1995, South Carolina's ethics board found that system operators' accessibility to unencrypted electronic mail might be sufficient to waive the privilege absent some mechanism to ensure confidentiality.[24] Under its analysis, absent certain confidentiality, e-mail communication with a client was impermissible absent express client waiver.[25] The committee noted that "the very nature of online services was such that the system operators of the online service may gain access to all communications that occur on the online service" and therefore required client consent to pass privileged information via the Internet.[26] As critics of limited privilege rightly point out, however, this might not have been an accurate statement of the law: "the logic of the opinion would apply to land line telephone hookups, because telephone companies employ system operators at their switches and other facilities."[27]

In 1996, an Iowa opinion also required encryption or client consent to send "sensitive material" via the Internet.[28] At about the same time, Colo-

---

21. N.Y. C.P.L.R. § 4548 (McKinney 1999) (originally enacted as § 4547 and renumbered in 1999).

22. Kevin J. Connolly, *Cryptography Can Ensure E-mail Confidentiality*, 19 NAT'L L.J. 41, at B13 (Jun. 9, 1997).

23. *See* discussion of ECPA, *infra* at Part IV.C.

24. *See* James K. Lehman, *Litigating in Cyberspace: Discovery of Electronic Information*, S.C. LAW., Apr. 1997, at 14, 15, 17 (citing S.C. Bar, Advisory Op. 94-27 (1995)).

25. *See* Joan C. Rogers, *Ethics, Malpractice Concerns Cloud E-mail, Online Advice*, 12 Law. Man. on Prof. Conduct (ABA/BNA) 59, 60-61 (Mar. 6, 1996) (citing S.C. Bar, Advisory Op. 94-27 (1995)).

26. William Freivogel, *Internet Communications—Part II, A Larger Perspective*, ALAS LOSS PREVENTION J., Jan. 1997, at 2 (quoting S.C. Bar, Advisory Op. 94-27 (1995)).

27. *See id.*

28. Iowa Supreme Court Board of Professional Ethics and Conduct Op. 96-1 (1996).

rado warned attorneys that they must ensure e-mail confidentiality to prevent waiver of the privilege,[29] and Arizona stated that encryption should be used when e-mailing confidential information.[30] Furthermore, Massachusetts, New York City, and New Hampshire ethics boards stated that use of cellular phones would not maintain the privilege.[31] Given the frequent analogies made between cellular telephony and unencrypted Internet electronic mail, it would hardly have been surprising if those entities had released similar statements regarding e-mail over the Internet.

As the decade drew to a close, however, ethics board opinions grew uniformly optimistic. In 1997, South Carolina re-examined its earlier policy "in light of the current state of technology."[32] The new opinion found that although the earlier opinion had been correct, because of the now-commonplace use of electronic mail, "improvements in technology and changes in the law" had created "a reasonable level of 'certainty' and expectation that such communications may be regarded as confidential."[33] Other than the increased popularity of e-mail, however, these putative changes seem like distinctions without a difference. The "changes in the law" discussed were limited to the 1994 amendments to ECPA,[34] which were implemented prior to the 1995 publication of the original South Carolina opinion.[35] Perhaps more striking was that the "improvements in technology," which allegedly justified this new opinion, were never detailed or described. By 1998, Alaska,[36] New York State,[37] and Vermont[38] had followed suit, finding that ECPA's protection and questionable analogies between electronic mail and voice telephony sufficed to ensure applicability of the privilege. Uniformly, these opinions cited the same few

---

29. *See* Victoria Slind-Flor, *Defense Bar Misses a Good Show on High Tech*, NAT'L L.J., Oct. 14, 1996, at A6.

30. *See* Susan B. Ross, *E-mail: How Attorneys Are Changing the Way They Communicate*, C. HILL LEGAL PRAC. NEWSL. (page unavailable) (July 1996), *available at* <http: //www.interlegal.com/1artcollege.html>.

31. *See* Rogers, *supra* note 25, at 61.

32. South Carolina Bar Advisory Op. 97-08 (1997), *available at* <http://www.scbar.org/apps/reference/EthicsOpinions/ ethicsopinion.dbm?OpinionID=97%2D08&OpinionType=ethics>.

33. *Id.*

34. Pub. L. No. 103-322, 108 Stat. 2147 (1994).

35. ECPA's putative role in privilege analysis is discussed *infra* Part IV.B.2.

36. *See* Alaska B. Ass'n, Ethics, Op. 98-2 (1998) (on communication by electronic mail), *available at* <http://www.alaska.net/~akctlib/eo98-2.txt>.

37. *See* New York St. B. Ass'n Committee on Professional Ethics, Op. 709 (1998), *available at* <http://www.nysba.org/opinions/Opinion709.html>.

38. *See* Vermont B. Ass'n Comm. on Professional Responsibility, Advisory Op. 97-5 (1997), *available at* <http:www.vtbar.org./AdvisoryEthicsOpinions/1997/97.05htm>.

sources: articles from law journals, practitioners' newspapers, and the ECPA. Finally, in 1999, the ABA Standing Committee on Professional Ethics weighed in.[39] As discussed in the Introduction, its opinion differed from those that preceded it only in degree, and it too found that unencrypted e-mail could support the privilege.

B. The Confidentiality Requirement and Contemporaneous Intent

Confidentiality is the measure of contemporaneous intent to keep a communication secret. "A communication is in confidence ... if, at the time and in the circumstances of the communication, the communicating person reasonably believes that no one will learn the contents of the communication except a privileged person."[40] Wigmore's classic enumeration of its limits is reasonably clear. "'The moment confidence ceases,' said Lord Eldon, 'privilege ceases.' This much is universally conceded."[41] Lack of confidentiality will deny applicability of attorney-client privilege because "the privilege is not violated by receiving such disclosures as the client by his own will permits to be made."[42] Moreover, "the mere relation of attorney and client does not raise a presumption of confidentiality, and the circumstances are to indicate whether by implication the communication was of a sort intended to be confidential. These circumstances will of course vary in individual cases, and the ruling must therefore depend much on the case in hand."[43]

Because the privilege is an exception to the rule requiring testimony, third parties who obtain knowledge of privileged communications are not thereby bound.[44] Possession of information by third parties has presumptively indicated unprivileged status, although the presumption may be rebutted by proof of theft or deceit.[45]

The intended confidentiality must have been both subjective and objective.[46] In most jurisdictions, the client must have subjectively intended that the communication be confidential, and no transmission to a third party attempted; whether that third party in fact receives the communica-

---

39. ABA Op., *supra* note 1.

40. RESTATEMENT, *supra* note 7, § 121.

41. WIGMORE, *supra* note 6, § 2311, at 599 (footnote omitted).

42. *Id.* § 2327, at 634.

43. *Id.* § 2311, at 600 (footnotes omitted).

44. *See id.* at 601-03.

45. *See* William P. Matthews, Comment, *Encoded Confidences: Electronic Mail, the Internet, and the Attorney-Client Privilege*, 45 U. KAN. L. REV. 273, 281 (1996) (citing PAUL R. RICE, ATTORNEY-CLIENT PRIVILEGE IN THE UNITED STATES § 9:26, at 681 (1993)).

46. *See* Rose, *supra* note 11, at 184.

tion is irrelevant.[47] Objectively, the client's expectation of confidentiality must have been reasonable under the circumstances. It cannot have been made in the presence of a third party, unless that person is an agent of the client or attorney, a joint client, or a joint defendant.[48]

Confidentiality requires reasonable protection against willful eavesdropping.[49] "[I]t is not asking too much to insist that if a client wishes to preserve the privilege ... he must take some affirmative action to preserve confidentiality."[50] Interception of a message intended to be kept confidential may result in loss of privilege.[51] However, the trend appears to be in favor of analyzing both the protective measures taken and the circumstances of interception,[52] or toward requiring intent.[53] Furthermore, the ECPA may protect the privilege in certain circumstances.[54]

C. The Non-Waiver Requirement[55]

While confidentiality depends on contemporaneous intent to maintain secrecy of a communication, waiver is a measure of a privileged party's subsequent efforts to maintain the privilege.[56] Because few parties intentionally and overtly waive the privilege, the issue before a court faced with a conflict over the existence of waiver tends to become "[w]hat constitutes a *waiver by implication*."[57]

> Judicial decision gives no clear answer to this question. In deciding it, regard must be had to the double elements that are predicated in every waiver, i.e., not only the element of implied intention, but also the element of fairness and consistency. A

---

47. *See id.* at 184-85. However, certain jurisdictions, such as New York, depart from this rule. The New York Court of Appeals has held that communications created by a potential defendant to be sent to non-attorneys, but which were prevented from delivery, were protected in a criminal prosecution. *See, e.g., In re* Vanderbilt, 439 N.E.2d 378 (N.Y. 1982).

48. *See* Rose, *supra* note 11, at 185.

49. *See In re* Grand Jury Proceedings, 727 F.2d 1352, 1356 (4th Cir. 1984).

50. *In re* Horowitz, 482 F.2d 72, 81 (2d Cir. 1973), *cert. denied*, 414 U.S. 867 (1973).

51. *See* Arthur L. Smith, *E-mail and the Attorney-Client Privilege* (visited Dec. 2, 1999) <http://www.bamsl.org/lpm/email.htm>.

52. *See id.*

53. *See* Daniel J. Pope & Helen Whatley Pope, *"Is It Safe..."*, 64 DEF. COUNS. J. 138, 141 (1997).

54. This idea is analyzed at some length in the discussion of ECPA, *infra* Part IV.C.

55. A discussion of various waiver approaches can be found in *Bank Brussels Lambert v. Credit Lyonnais (Suisse) S.A.*, 160 F.R.D. 437 (S.D.N.Y. 1995).

56. *See,* WIGMORE, *supra* note 6, § 2327, at 634-38.

57. *See id.* at 635 (emphasis in original).

> privileged person would seldom be found to waive, if his intention not to abandon could alone control the situation. There is always also the objective consideration that when his conduct touches a certain point of disclosure, fairness requires that his privilege shall cease whether he intended that result or not.[58]

Failure to take appropriate measures to maintain subsequent confidentiality will waive the privilege. For example, a corporation that cannot demonstrate that privileged documents were maintained in a reasonably secure location where access was controlled may find that it has implicitly waived the privilege.[59]

Intent to maintain confidence may not be presumed for privilege purposes.[60] Indeed, because messages "[are] frequently disclosed to persons 'outside the circle of confidentiality'" by a recipient's decision to forward them, the burden of proof as to intent of confidentiality may be greater for e-mail than for other means of communication.[61]

Waiver can be effected by the client or its agent so authorized—and that authorized agent may be its attorney.[62] In *Commodity Futures Trading Commission v. Weintraub*,[63] the Supreme Court found that the ability to waive in the corporate context is usually limited to the corporation's "control group":[64] those corporate personnel "in a position to control or even to take a substantial part in a decision about any action which the corporation may take upon the advice of the attorney."[65] It did so notwithstanding *Upjohn*'s specific abolition of the use of the test to limit the privilege to control group speakers.[66] However, *Weintraub* has been interpreted in at least one court as applying only under bankruptcy; otherwise, the fact that communications by non-control group employees enjoy the privilege permits those same employees to waive through voluntary disclosure.[67]

---

58. *See id.* at 635-36 (footnote omitted).

59. *See* Smith, *supra* note 51.

60. *See* WIGMORE, *supra* note 6, § 2311, at 599-603.

61. Susan J. Silvernail, *Electronic Evidence: Discovery in the Computer Age*, 58 ALA. LAW. 176, 179 (1997).

62. *See* Rose, *supra* note 11, at 187.

63. 471 U.S. 343 (1985).

64. *See id.* at 348.

65. Upjohn Co. v. United States, 449 U.S. 383, 390 (1981) (quoting Philadelphia v. Westinghouse Electric Corp., 210 F. Supp. 483, 485 (E.D. Pa. 1962)).

66. *See id.*

67. *See* Jonathan Corp. v. Prime Computer Inc., 114 F.R.D. 693 (E.D. Va. 1987).

Waiver of the privilege is rarely express, but rather implied by conduct that would make its application unfair.[68] Waiver may occur where a third party has not read or heard the communication, but could have.[69] "Waiver of the privilege has been found where documents were stored in a place accessible to third parties, placed in a public hallway for delivery to an attorney, ... left on a table in another person's hotel room, ... [and] kept in files routinely viewed by third parties."[70] In short, the carelessness demonstrated by making confidential information available to persons to whom the privilege does not apply can vitiate its application, whether or not confidentiality is actually compromised.

When the content of confidential communications is in fact learned by third parties without permission, primarily via eavesdropping or theft, the approaches taken by courts vary. Some courts do not treat such inadvertent disclosure as waiver when certain factors are present, including "the reasonableness of the precautions to prevent inadvertent disclosure, the time taken to rectify the error, the scope of the discovery and the extent of the disclosure."[71] Nonetheless, others insist that inadvertent disclosure constitutes waiver per se.[72] "[T]he majority of jurisdictions ... consider the circumstances surrounding [an inadvertent] disclosure and determine on a case-by-case basis whether [the] disclosure waives the attorney-client privilege."[73]

Reasonable precautions to protect the privilege are not necessarily foolproof; the fact that inadvertent disclosure has occurred does not indi-

---

68. Rose, *supra* note 11, at 188-89.

69. First Interstate Bank v. Nat'l Bank & Trust Co., 127 F.R.D. 186, 189 (D. Or. 1989).

70. Rose, *supra* note 11, at 190-91 (citing, respectively, *In re* Horowitz, 482 F.2d 72, 82 (2d Cir. 1973), *cert. denied*, 414 U.S. 867 (1973); *In re* Victor, 422 F. Supp. 475, 476 (S.D.N.Y. 1976); Bower v. Weisman, 669 F. Supp. 602, 605-06 (S.D.N.Y. 1987); Jarvis, Inc. v. American Tel. & Tel. Co., 84 F.R.D. 286 (D. Colo. 1979)).

71. Lois Sportswear, U.S. v. Levi Strauss & Co., 104 F.R.D. 103, 105 (S.D.N.Y. 1985).

72. *See, e.g.*, *In re* Sealed Case, 877 F.2d 976, 980 (D.C. Cir. 1989); Golden Valley Microwave Foods Inc., v. Weaver Popcorn Co., 132 F.R.D. 204, 208-09 (N.D. Ind. 1990); Underwater Storage Inc. v. United States Rubber Co., 314 F. Supp. 546, 549 (D.D.C. 1970).

73. Mary Frances Lapidus, *Using Modern Technology to Communicate with Clients: Proceed with Caution and Common Sense*, HOUS. LAW., Sept./Oct. 1996, at 39, 40 n.41 (citing Alldread v. City of Grenada, 988 F.2d 1425 (5th Cir. 1993); Granada Corp. v. First Court of Appeals, 844 S.W.2d 223 (Tex. 1992)).

cate unreasonableness per se. However, disclosures due to "extreme or gross negligence" may be deemed intentional.[74]

III. UNDERSTANDING ELECTRONIC MAIL

New technologies have changed the practice of law before—air travel, overnight mail, facsimile transmission, and online information services like Lexis and Westlaw, to name a few.[75] Now, electronic mail has taken root in law firms and in their clients' businesses, and technology is once again changing the practice of law.

> E-mail is the most popular Internet application, and the most used by lawyers, because it enables rapid, efficient communication and file sharing with anyone in the world from the lawyer's desk. The practice of law is dependent upon the rapid transmission of information and documents over geographical space, and time deadlines and sensitive documents make e-mail and its associated applications the fastest growing form of communications for lawyers. The lawyer of 2010 will use electronic [mail] as often as the telephone or letter today.[76]

The popularity of e-mail has grown despite fears about security because computer files generally, and electronic mail specifically, have significant advantages in speed, cost, storage, rapidity of access, ease of searching, and the ability to reuse portions without retyping.[77]

A. E-mail and the Dangers of Discovery

The increasing ubiquity of electronic mail potentially presents a trove of evidence which must be turned over in discovery. *In re Brand Name Prescription Drugs Antitrust Litigation*[78] upheld a discovery request for approximately 30 million pages of e-mail, despite protests that it would cost at least $50,000 to comply. In that case, the court found that "if a party chooses an electronic storage method, the necessity for a retrieval program or method is an ordinary and foreseeable risk."[79] Two aspects of

---

74. *Id.* (citing FDIC v. Marine Midland Realty Corp., 138 F.R.D. 479, 482 (E.D. Va. 1991)).

75. *See* Pope & Pope, *supra* note 53, at 138.

76. Richard M. "Rick" Georges, *The Impact of Technology on the Practice of Law—2010*, FLA. B.J., May 1997, at 36, 38.

77. *See, e.g.*, Robert L. Jones, *Client Confidentiality: A Lawyer's Duties with Regard to Internet E-mail* (Aug. 16, 1995) <http://www.computerbar.org/netethics/bjones.htm>; Ross, *supra* note 30.

78. 1995 WL 360526 (N.D. Ill. June 15, 1995).

79. *Id.* at 1.

electronic mail make its potential discovery particularly dangerous: its informality and its persistence.

1. *Informality of Electronic Mail*

Numerous commentators have noted the informality of electronic mail,[80] which can lead to dissemination of information traditionally transmitted by telephone or in person rather than through the permanent medium of office memoranda.[81]

> E-mail users often perceive their correspondence as ephemeral and, accordingly, do not exercise discretion in their communications.... The most important concern for companies is that employees all too frequently use casual, off-the-cuff language in their e-mail messages, quite unlike what they would write in ordinary business correspondence.[82]

As one expert notes, "It's as if people put their brains on hold when they write e-mail. It's a substitute for a phone call, and that's the danger"[83]—that is, users treat it as if it maintains no records of communications. Because little, if any, thought is given to the record left behind when sending an e-mail, the risk of creating a record of decontextualized statements is increased.[84]

It is not surprising that, since as "a substitute for telephonic[,] printed[, and] direct oral communications, ... e-mail has become an indispensable tool in the work place, it has also become the 'digital smoking gun' in more and more lawsuits."[85]

---

80. *See, e.g.*, Georges, *supra* note 76, at 38 ("Communication by e-mail is not as formal as written correspondence, nor as informal as speech."); Bramesco, *supra* note 15, at 527 ("E-mail messages tend to be conversational, brief and 'folksy.'")

81. *See* Michael Traynor, *E-mail Authentication Is Key*, NAT'L L.J., Aug. 1, 1994, at B9. *See also* Charles R. Merrill, *Toward a Paperless Federal Practice by the Year 2000*, 484 PLI/PAT 125, 130 (1997) ("[T]here is a tendency to use [e-mail] for internal conversations which would formerly have taken place in-person or by phone, and for external conversations which would formerly have taken place by phone.").

82. Charles A. Lovell & Roger W. Holmes, *The Dangers of E-mail: The Need for Electronic Data Retention Policies*, R.I. B.J., Dec. 1995, at 7.

83. Leslie Helm, *The Digital Smoking Gun: Mismanaged E-mail Poses Serious Risks, Experts Warn*, L.A. TIMES, June 16, 1994, at D1 (quoting John H. Jessen of Electronic Evidence Discovery, Inc.).

84. *See* Lehman, *supra* note 24, at 15.

85. Silvernail, *supra* note 61, at 181; *see also* Lovell & Holmes, *supra* note 82, at 7 ("[P]laintiffs' attorneys increasingly view e-mail as a source of 'smoking gun' evidence waiting to lead to painful revelations and, possibly large settlements.").

2. *Persistence of Electronic Mail*

Unlike the telephone, which typically generates only transactional information, e-mail leaves records of its content. Even deleted e-mail messages often can be retrieved indefinitely from a computer system.[86] The indefinite life expectancy of e-mail has resulted in discovery requests by attorneys which ask for "deleted" e-mail messages and hard drives. Even computer system employees are now asked to attend depositions.[87] The problem is compounded by the fact that while there tends to be a significant correlation between multiplicity of printed copies and lack of intended confidentiality, the same does not necessarily apply to electronic media.[88]

> Use of backups to protect data integrity makes deletion inherently more difficult. Companies use digital storage systems because they offer an inexpensive and space saving alternative to traditional paper storage. This results in an exponential increase in the amount of discoverable information available during litigation. This information may include potentially damaging documents thought to have been destroyed years ago.[89]

Stored electronic mail is discoverable under Federal Rules of Civil Procedure 26(a)(1)(B) and 34.[90] To actually permanently destroy e-mail, the author and all recipients must delete it, and all backups must be erased or overwritten.[91] Absent applicable legislation or rulemaking, an appropriate balance adopted by practitioners is to use phone or in-person communications when disclosure of the content of the communications could be potentially damaging.[92] When such inherently evanescent forms of com-

---

86. *See* Bramesco, *supra* note 15, at 527; *see also* Lovell & Holmes, *supra* note 82, at 8; Charles R. Merrill, *E-mail for Attorneys from A to Z*, N.Y. ST. B.J., Jun. 1996, at 20, 23 (1996); Silvernail, *supra* note 61, at 180-181 ("Electronically stored records are not as easily destroyed as paper records. Contrary to conventional wisdom, when a user strikes the 'delete' key, the data is [sic] not physically removed from the hard drive.... The data remains [sic] undisturbed until more space is needed on the hard drive.").

87. *See* Bramesco, *supra* note 15, at 527.

88. A corporate employee sending a private memorandum to corporate counsel will ordinarily not make several additional copies, while sending the same information by electronic mail will often inherently create such copies.

89. *See* Betty Ann Olmsted, *Electronic Media: Management and Litigation Issues when "Delete" Doesn't Mean Delete*, 63 DEF. COUNS. J. 523, 523 (1996); *see also* Lehman, *supra* note 24, at 15 (explaining that electronic communications can result in keeping backup copies, both intentionally and unintentionally).

90. *See* Merrill, *supra* note 83, at 130.

91. *See id.*

92. *See id.*

munication are undesirable or unavailable, encrypted e-mail should be considered as an appropriate alternative.

B. Encryption[93]

1. Cryptography 101

A brief introduction to cryptography and the terminology surrounding it may be of use. Cryptography is the use of "difficult problems" to alter information, the solution to which requires "secret knowledge"—usually referred to as a cryptographic key. Encryption, a practical application of cryptography, is "the transformation of data into a form that is [practically] impossible ... to read without ... appropriate knowledge (a key)."[94] Cryptography ensures privacy because access to the encrypted communication does not provide access to its contents. It therefore permits secure transfer of information over an insecure medium.

Electronic mail can use encryption to secure communications, ensuring that unwanted third parties cannot comprehend them. It can also be used for identification and authentication of parties to a communication, verifying parties' identities in much the same way as an ATM personal identification number. Generally, managing the transfer, storage, and authentication of keys is the largest deterrent to acceptance of encryption in the workplace.

There are two primary types of encryption: symmetrical key[95] and public key.[96] Symmetrical-key encryption is the traditional variety, in which the same key is used both to encrypt and decrypt a message. However, large-scale practical application of symmetrical key encryption tends to fall victim to the "key transfer problem." The parties to the communication must agree on the key to be used, and that agreement must be done secretly. As a practical matter, the coordination necessary to transfer the secret key securely is often difficult if not impossible, in that appropriate security requires both authentication of the desired parties and exclusion of others.

---

93. The discussion of encryption technology and cryptography in this section is based on the author's personal knowledge. For additional sources on cryptography and encryption, see generally A. Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709, 885-97 (1995) and RSA LABS., FREQUENTLY ASKED QUESTIONS ABOUT TODAY'S CRYPTOGRAPHY (4th ed. 1998), *available at* <ftp://ftp.rsasecurity.com/pub/labsfaq/labsfaq4.pdf> (PDF file).

94. RSA LABS., *supra* note 93, § 1.2, at 10.

95. Also referred to as "secret" or "private."

96. Also referred to as "asymmetrical."

A breakthrough arrived in the late 1970s with the advent of public-key encryption. Public-key encryption solves the key transfer problem by allowing the use of different keys by the sender (to encrypt) and the recipient (to decrypt). Two keys, such as extremely large prime numbers, relate formulaically such that what is encrypted with one may only be decrypted with the other, and the identity of one cannot be practicably derived from knowledge of the other. Because public-key encryption avoids key transfer issues, it can be used to create a widely-deployed cryptographic infrastructure.

As a practical matter, preparing to use public-key encryption is fairly simple. A user obtains appropriate software, such as Pretty Good Privacy ("PGP").[97] The user then generates a key pair, keeping one key secret and marking the other for public distribution. The secret key is usually encrypted by symmetrical encryption using some secret "passphrase" to prevent someone who gains access to it from being able to use it, but there is no key transfer problem because that key is intended only for the use of one person. The association of the public key with the user is then authenticated by a trusted third party called a certification authority ("CA"), which makes the key publicly available and vouches for its validity.

Using public-key cryptography to encrypt electronic mail typically entails several steps, most of which are transparent to the user. First, the author creates an unencrypted message ("plaintext"), and tells her encryption software to encrypt that message and send it to the intended recipient or recipients. At this point, the encryption software takes over, and operations become opaque to the user. The software attempts to find the recipient's public key in its local key directory; if it is not found, the software requests the recipient's key from a trusted CA, which may in turn request the key from other CAs. The software then generates and uses a single-use secret key to encrypt the message. Then the software encrypts the session key using the recipient's public key, so that only the recipient can decrypt the message. Finally, the software sends both the message (encrypted with the session key) and the session key (encrypted with the recipient's public key) via an insecure network such as the Internet.

The recipient's decryption software follows a parallel process. If the electronic mail software is suitably automated, it recognizes that an encrypted message has been received; otherwise, the user must request de-

97. PGP was the first commonly-available implementation of asymmetrical cryptography in end-user software. With over 6 million users, it has become the de facto standard for message encryption. *See* Network Assoc., *PGP Total Network Security—PGP Encryption & PKI* (visited Oct. 17, 1999) <http://www.nai.com/asp_set/products/tns/pgp_freeware.asp>.

cryption. Either way, the software first verifies that the session key was encrypted with a public key with a corresponding private key that is available to the user. Then the software requests that the recipient provide an appropriate passphrase to decrypt the stored private key. Assuming that the passphrase is entered correctly, the encryption software uses the private key to decrypt the session key, then uses that decrypted session key to decrypt the actual message. That message is then displayed as the original plaintext.

Using public-key cryptography for authentication of electronic mail—commonly called digital signatures—is essentially the reverse of using it for encryption. In public-key cryptography, that which is encrypted with one key of a related pair can only be decrypted with the other, and vice versa. Thus, if a message may be decrypted with the public key, it must have been encrypted with the private key. If that private key has been kept secret, that ensures that the communication came from the user in question.

Properly implemented, a public-key cryptosystem provides practically absolute confidentiality.[98] In fact, there are more possible combinations of public-private key pairs used in typical implementations of RSA[99] than there are atoms in the known universe.[100] Any form of security can be compromised; military-grade public-key cryptography is no exception. "Public-key cryptography may be vulnerable to impersonation," wherein an interceptor tricks the sender into using the wrong public key.[101] Furthermore, individual messages may be cracked through brute force—trying every possible key until one works—and hackers can intercept them pre-encryption or post-decryption.[102] However, as part of a systematic approach to security, properly-implemented cryptography provides extremely high levels of protection.[103] In fact, encrypted electronic mail may be the most confidential interpersonal communications medium available, and its use may indicate presumptive intent to maintain confidentiality for attorney-client privilege purposes.

Indeed, much of the fear over the potential lack of protection for unencrypted e-mail appears to have been generated by the presence of such an

---

98. *See, e.g.*, RSA LABS., *supra* note 93, § 3.1.3 at 61.

99. RSA, named after inventors—Ronald L. Rivest, Adi Shamir, and Leonard M. Adelman—is the most commonly used asymmetric encryption algorithm. It is described by U.S. Patent No. 4,405,829 (issued Sept. 20, 1983).

100. *Id.* § 3.1.6 at 64.

101. *Id.* § 2.1.3 at 20.

102. *See* Freivogel, *supra* note 26.

103. *See* Jones, *supra* note 77.

ironclad alternative. Because available encryption mechanisms provide essentially invulnerable protection, courts might be persuaded that failure to use encryption waives the privilege.[104] Some commentators have noted that in *The T.J. Hooper*,[105] Learned Hand, writing for the Second Circuit, found negligence in failure to use available technology that was not yet in widespread use. Likewise, "Hand's Formula," announced in *United States v. Carroll Towing*,[106] states that if the potential for loss multiplied by the magnitude of that loss exceeds the burden required to prevent it, the failure to take preventive measures constitutes negligence.[107] Neither *The T.J. Hooper* nor *Carroll Towing* has been cited to overcome the attorney-client privilege.[108]

One commentator has noted that if the burden of encryption is sufficiently light, failure to use it may be found negligent without knowing the likelihood of electronic mail interception.[109] However, his analysis considered only the out-of-pocket expenditure required to purchase a license to use PGP. In fact, the cost of the software may be the least burdensome aspect of e-mail encryption.

2. *Barriers to Effective Implementation of Encryption*

Despite the obvious security benefits of using encryption software, there are practical barriers to implementing encryption for interorganizational communication, such as the requirement of uniform or interoperable software,[110] limited exportability,[111] key management,[112] and ease of use.[113] Nonetheless, these problems can be solved. Software interoperability has become possible through implementation of appropriate standards for interapplication communication.[114] Export limitations are not a barrier to most American attorneys, and less secure versions of cryptographic products are available for export.

---

104. *See* Pope & Pope, *supra* note 53, at 143.
105. 60 F.2d 737 (2d Cir. 1932).
106. 159 F.2d 169 (2d Cir. 1947)
107. *See id.* at 173.
108. *See* Freivogel, *supra* note 26.
109. *See* Jones, *supra* note 77.
110. *See id.*
111. *See* Albert Gidari, *Privilege and Confidentiality in Cyberspace*, COMPUTER LAW., Feb. 1996, at 1, 3.
112. *See id.*
113. *See* Ross, *supra* note 30.
114. *See* David Willis, *Secure Electronic-Mail: Return To Sender?*, NETWORK COMPUTING, Nov. 1, 1997, at 108; *see also* Ronald V. Grant, *Law Office Technology*, HAW. B.J., Jun. 1997, at 24.

Though e-mail is considered a personal technology, centralized control of encryption keys is critical in the corporate e-mail environment in order to maintain the corporation's assets.[115] If each user possesses a different private key, the firm can get blocked from access to information it or its client owns. Central key management is therefore necessary to ensure that the corporation or law firm owns the relevant cryptographic keys.[116]

The administration of a company's encryption system is admittedly non-trivial.[117] Specifically, problems of access by the company to employee keys have been formidable. However, these administration problems are being addressed. Certain products allow certificates to contain separate keys for encryption and signatures, so that the individual user is the only person with control over her signature, but the firm can have access to any encrypted materials.[118] Even PGP, historically the most individual-oriented public-key cryptosystem, has made increasing allowances for business users. By automatically sending an encrypted blind carbon copy of all encrypted messages to a central electronic "drop box," encryption policy enforcement software can ensure that the corporation or law firm's management can gain access to the contents of encrypted communication without involving the individual user.[119] This same software can also enforce different policies for different groups of users. For instance, it may require encryption for messages sent by a client's legal department to its outside counsel, while allowing the marketing department to send unencrypted mail.[120]

Despite their technical significance in development of an integrated public-key infrastructure,[121] key management risks are often negligible as a practical matter in any given communication. "With good encryption, your only security risks come from someone stealing the private encryption keys, or someone tricking you into thinking he's your client [or another intended recipient].... You're probably more likely to send a fax to

---

115. *See* Willis, *supra* note 114, at 108.

116. *See* Rogers, *supra* note 25, at 65.

117. *See* Jones, *supra* note 77 (citing BRUCE SCHNEIER, E-MAIL SECURITY 41 (1995)).

118. *See Securing Electronic-Mail Across Borders*, NETWORK COMPUTING, Nov. 1, 1997, at 112.

119. *See* Willis, *supra* note 114, at 116.

120. *See* Larry Stevens, *Mac Encryption Finding Its Way Into Corporations*, MACWEEK, Oct. 27, 1997, at 16 (describing corporate use of encryption software).

121. Such an infrastructure would provide for secured electronic transactions, both financial and informational, and is seen as a primary mechanism to further develop the Internet and other network technologies.

the wrong number by accident than you are to have someone trick you with a *doppelgänger* encryption key."[122]

The ease of use of encryption software has also improved greatly over recent years. In the past, this software was "still somewhat cumbersome to use,"[123] but more recent versions integrate into popular e-mail programs, making "encrypting sensitive messages as easy as automatic transmission makes driving a car."[124] Today, the most popular Internet mail clients, including Qualcomm's Eudora and Microsoft's Outlook series, now integrate seamlessly with cryptographic software. For instance, when composing a message in Eudora with PGP installed, two new icons are placed just under the right of the message's title bar, one for encryption and one for digital signatures. Rather than writing a message in one program, launching the encryption software, and telling the software to encrypt and/or sign the message, the user need simply click on the appropriate icon. The software handles the remainder of the process; assuming that it can find the recipient's public key, no further intervention by the sender is required.

Admittedly, the network administrator's job continues to be complex even though the user's job is no longer difficult. On a technical level, the administrator must make appropriate arrangements with CAs and configure any policy enforcement software. Furthermore, because introducing new software into a networked environment almost always threatens to upset a delicate equilibrium, administrators are usually justifiably reluctant to suggest additional functionality. As a practical matter, the administrator must also obtain funding for purchase and implementation of encryption technologies and overcome bureaucratic inertia. Depending on management priorities, that funding may come at the expense of other services.

All told, then, deploying a cryptographic infrastructure is hardly a trivial task. Because much of a network administrator's time is dedicated to remedying existing problems, she may be justifiably reluctant to raise another. However, assuming appropriate support from relevant management, these barriers can—and should—be overcome.

---

122. G. Burgess Allison, *Technology Update*, L. PRAC. MGMT., Apr. 1996, at 16, 20.

123. Ross, *supra* note 30 (discussing PGP).

124. Samuel Lewis, *Memoirs From the Corner Suite: An Update on Security and the Internet* (last modified Mar. 24, 1997) <http://www.collegehill.com/ilp-news/lewis2.html>.

IV. SECURITY ISSUES ATTENDANT TO INTERNET ELECTRONIC MAIL

Misinformation about Internet security issues is unfortunately the norm, even among those who should be well-informed.[125] It creates misguided legal commentaries that quickly conclude that unencrypted e-mail will maintain the attorney-client privilege. Analyzing the privilege's application to e-mail requires genuine knowledge of the technology. To dismiss the technological sophistication of the issue, as several commentaries have, creates an expectation regarding the privilege among the legal community that may be proven incorrect when the issue is addressed by a court.

Much of the misinformation used in legal commentaries can be grouped into three areas of ignorance: closed networks provide a solution to privilege issues that is unattainable on the Internet; laws criminalizing interception of network traffic protect the privilege; and analogies between Internet electronic mail and other means of communications dictate application of the privilege. A look at each of these areas indicates that those legal opinions asserting that attorney-client privilege necessarily applies to e-mail may be less conclusive than the opinions suggest.

A. Closed Networks Versus the Internet

Private commercial networks like CompuServe and Lexis' Counsel Connect are unquestionably safer than the Internet, because their traffic is regulated by a single entity.[126] Therefore, case law supports the proposition that a user has a reasonable privacy interest in electronic mail sent

---

125. Take Charles R. Merrill, for instance. Merrill "heads [McCarter & English's] Computer and High Tech Law Practice Group[,] ... [s]erves as National Moderator of the Lexis Counsel Connect E-mail and Electronic Commerce Forum, and is Co-Rapporteur of the Digital Signature Guidelines, a project of the ABA Information Security Committee, Section of Science and Technology." Charles R. Merrill, *E-mail for Attorneys from A to Z*, 443 PLI/PAT 187, n.1 (Dec. 1996). Yet Merrill misstates that secure socket layer ("SSL") technology would be available "probably within the next twelve months." Merrill, *supra* note 86, at 23. In fact, it had been in place for at least a year prior to publication of his article. He also claims that SSL provides a mechanism to secure interaction between SMTP-compliant e-mail servers, when in reality, it applies only to communications between web servers and browsers. He is also incorrect to claim, as do others, that private commercial internetworks like "ATTMail, MCIMail, Sprint, Compuserve, AOL, Prodigy, Lexis Counsel Connect" provide added security via use of circuit-switched connections rather than packet-switched ones. *Id.* In fact, all computer networks use packet-switched communications; the added security provided by private commercial networks is due to their total control over traffic.

126. *See* Grant, *supra* note 114, at 33-34.

over a single network, even one connected to the Internet.[127] E-mail sent over proprietary services is sufficiently secure, but that which travels through multiple systems—such as on the Internet—may be accessible to too many people to minimize risks.[128]

Yet the days of the closed private internetwork may be numbered, thanks to the seductive openness of the Internet, which allows internetwork communication almost as easily as intranetwork. What is gone is the need to establish dedicated links between attorney and client, or to agree on a common private commercial internetwork; gone also is the added security both solutions supply. "The shift from closed to open systems for computer networking raises several legal and legal automation issues that are worth thinking about in determining when and how lawyers should use the Internet in addition to or instead of closed information services."[129] However, public-key cryptography can remedy the privacy issues which inhere to public internetworks, such as the Internet.[130] Not only can cryptography secure e-mail between sender and recipient, it can be used to create "virtual private networks" of encrypted nodes over the public Internet.[131]

B. Misplaced Reliance on ECPA and Other Criminal Laws for Protection of Privilege

1. *The Electronic Communications Privacy Act of 1986 (ECPA) Criminalizes Interception of E-mail*

The ECPA protects "wire, oral, or electronic communications"[132] against warrantless interception by law enforcement officers,[133] and criminalizes such interception by other persons.[134] Many commenting on application of attorney-client privilege to electronic mail note one provision of ECPA, which provides that "[n]o *otherwise privileged* wire, oral, or elec-

127. *See, e.g.,* United States v. Maxwell, 45 M.J. 406 (C.A.A.F. 1996) (finding Fourth Amendment privacy interest in e-mail sent over America OnLine's network).

128. *See* Smith, *supra* note 51.

129. Henry H. Perritt, Jr., *Security in Open Networks: Maintaining Confidentiality and Getting Paid* (visited Sept. 24, 1999) <http://www.cilp.org/chron/articles/pbisecu6.htm> (footnote omitted).

130. *See* Merrill, *supra* note 85, at 128.

131. *See, e.g.,* Mike Fratto, *The State of Security 2000* (Oct. 4, 1999) <http://www.nwc.com/1020/1020f22.html> (discussing virtual private networks).

132. 18 U.S.C.A. § 2517(4) (West 1999).

133. *See* 18 U.S.C.A. § 2516 (1982) (amended 1994).

134. *See* 18 U.S.C.A. § 2511(1982) (amended 1994).

tronic communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character."[135]

Some commentators have argued that because ECPA's protection for electronic mail is similar to that for telephone calls, the two should be treated similarly for privilege purposes.[136] For instance, system administrators of an "electronic services provider," like telephone company employees, may intercept communications when necessary for provision of service or to protect their property, pursuant to 18 U.S.C. § 2511(2)(a)(i).[137] However, it is unclear whether ECPA's "electronic services provider" provisions apply to Internet transmission.[138] Cases such as *State Wide Photocopy Corp. v. Tokai Financial Services, Inc.*[139] have found ECPA's electronic services provider provisions available only to entities that actually provide services to the public.[140] The limitations contained in ISP contracts and interconnection agreements may preclude application of ECPA,[141] as may the fact that some ISPs do not provide services to the public per se, but only to corporate entities.

No reported case considers the privilege impact of 18 U.S.C. § 2517(4)'s "otherwise privileged" language due to interception of attorney-client communications. The legislative history for the original ECPA legislation, prior to the 1986 amendment which added "electronic communication" to "wire or oral communication,"[142] states that 18 U.S.C. § 2517(4) "is intended to vary the existing law only to the extent it provides that an otherwise privileged communication does not lose its privileged character because it is intercepted by a stranger. Otherwise, it is intended to reflect existing law."[143] This fails to clarify the meaning of the section as to whether the privilege is compromised by the vulnerability of the me-

135. 18 U.S.C.A. § 2517(4) (1982) (amended 1994) (emphasis added).

136. *See, e.g.*, Flaming, *supra* note 13, at 184.

137. *Id.*

138. *See* Matthews, *supra* note 45.

139. 909 F. Supp. 137, 145 (S.D.N.Y. 1995) (application of ECPA denied because party does not "provide[] a communication service to the public, but ... is in the business of financing and ... merely uses fax machines and computers as necessary tools of almost any business today").

140. *See* Matthews, *supra* note 45, at 291.

141. *See id.* at 290-91. Service provider contracts commonly permit administrative interception by service provider employees, which is a loophole expressly provided in ECPA. *See id.* (citing 18 U.S.C. § 2511(2)(a)(i)).

142. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 101(c)(A) (1988). The Senate Report on ECPA, S. REP. NO. 99-541, *reprinted in* 1986 U.S.C.C.A.N. 3555, contains no specific references to privilege.

143. S. REP. NO. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112 (cases omitted).

dium per se to interception. All reported federal cases applying 18 U.S.C. § 2517(4) consider the effect of a wiretap executed as part of a criminal investigation on the privilege; none consider the effect of a communication's inherent lack of confidentiality.[144] However, some cases have denied application of the privilege to communications lawfully intercepted pursuant to wiretap,[145] despite the fact that 18 U.S.C. § 2517(4) provides that "[n]o otherwise privileged ... communication intercepted in accordance with ... the provisions of this chapter shall lose its privileged character."[146]

State analogues to ECPA also exist. Some states, including California, Connecticut, Georgia, Kansas, Michigan, Pennsylvania, and Texas, provide statutory protection against wiretapping.[147] However, at least one state—California—has found that those statutes do not apply to electronic mail,[148] while another—Texas—explicitly makes interception of e-mail illegal.[149]

2. *The ECPA Tautology: Criminality of Interception Mandates Applicability of Privilege*

Some commentators claim that ECPA's terms ensure the application of the privilege to unencrypted e-mail, regardless of the attendant common-law factors.[150] The line of reasoning is roughly as follows: Interception of telephone communications is illegal, and such interception does not preclude applicability of the privilege; since interception of computer

---

144. *See, e.g.*, United States v. Kahn, 415 U.S. 143 (1974), *rev'g* 471 F.2d 191 (7th Cir. 1972); United States v. Vastola, 899 F.2d 211 (3d Cir. 1990); Cruz v. Alexander, 669 F.2d 872 (2d Cir. 1982); United States v. Ford, 553 F.2d 146 (D.C. Cir. 1977); United States v. Hall, 543 F.2d 1229 (9th Cir. 1976); United States v. Feldman, 535 F.2d 1175 (9th Cir. 1976); United States v. Turner, 528 F.2d 143 (9th Cir. 1975); United States v. Kerrigan, 514 F.2d 35 (9th Cir. 1975).

145. *See, e.g.*, *Turner*, 528 F.2d 143 (wiretap orders entered lawfully under ECPA void attorney-client privilege as to intercepted communications); *Kerrigan*, 514 F.2d 35 (same); Commonwealth v. Alves, 608 N.E.2d 733 (Mass. 1993) (same as to spousal communications privilege).

146. 18 U.S.C.A. § 2517(4) (1982) (amended 1994).

147. *See* Matthews, *supra* note 45, at 292 (citing, *e.g.*, CAL. PENAL CODE §§ 630-632 (West 1986 & Supp. 1996); CONN. GEN. STAT. ANN. §§ 53a-187 to 53a-189 (West 1994); GA. CODE ANN. §§ 16-11-66 to 16-11-69 (1996); KAN. STAT. ANN. §§ 21-4001 to 21-4002 (West 1995); MICH. COMP. LAWS ANN. § 750.539d (West 1991); 18 PA. CONST. STAT. ANN. §§ 5705-5748 (1983 & Supp. 1996)).

148. *See id.*

149. *See* Lapidus, *supra* note 73, at 40.

150. *See, e.g.*, Freivogel, *supra* note 26; Gidari, *supra* note 115; Georges, *supra* note 77.

communications is also illegal, it must not preclude applicability of the privilege either.

Few are so blunt as the commentator who believes that absent contrary court findings, he may announce his own rule. "If the interception is criminal, the lawyer has not violated the ethics rules, has not waived any privilege, and has not subjected herself to civil liability. While we are not aware of any court stating such a rule in just that way, we are not aware of any decision that is contrary to it."[151] But he announces a few "obligatory *caveats*."[152] Some judges and ethics committee members lack comfort and familiarity with new technology. This may produce "occasional overreaction as a way of assuring that clients are protected," such as the "well-intentioned" Iowa and South Carolina opinions cautioning against faith in the privilege.[153] Furthermore, he finds one putatively anomalous case, *Suburban Sew 'n Sweep v. Swiss-Bernina*,[154] where waiver was found as to letters placed in a dumpster near the opposing party's loading dock. *Suburban Sew 'n Sweep* appears to adopt "the older, unforgiving approach to waiver favored by Wigmore," but it has not been cited to mean that commission of a crime in the obtaining of communications waives the privilege, and the subsequent passage of ECPA may deny its applicability as to electronic communications.[155] Most important, he admits, there are confidences so valuable that extraordinary measures must be taken to protect them.[156]

A similar tack is taken by another commentator.

> Fortunately, the law is not as muddled as conventional punditry suggests.... To understand the issue, we do not start with the Rules of Professional Conduct on maintaining the confidences and secrets of clients or with the technology or medium of exchange. Rather, we look to the criminal law.... [N]o one can lawfully intercept communications made over phone lines or wireless communications. The same is true for information or communications made over the Internet, including e-mail.[157]

---

151. Freivogel, *supra* note 26.

152. *Id.* (emphasis in original).

153. *Id.* (citing Iowa Supreme Court Board of Professional Ethics and Conduct Op. 96-1 (Aug. 29, 1996); South Carolina Bar Advisory Op. 97-08 (1997)).

154. 91 F.R.D. 254 (N.D. Ill. 1981).

155. Freivogel, *supra* note 26.

156. *See id.* However, Freivogel fails to note that protecting *all* communications might be an effective means to protect the extraordinary as well.

157. Gidari, *supra* note 111, at 1-2.

A third commentator is somewhat more cautious, despite asserting absolute non-waiver due to another's criminal conduct.

> As a result [of ECPA's prohibition on interception], it may be persuasively argued that e-mail communications to clients have the expectation of privacy, and that there is no waiver of the attorney-client privilege by their use.... For the same reason there is no privilege waiver when written mail is stolen, there is no privilege waiver when e-mail is intercepted by criminal conduct.... Even so, some authors postulate that the more prudent course of conduct is to encrypt all e-mail.[158]

Other commentators, however, take a different approach. That it is a crime to intercept e-mail is not necessarily sufficient to maintain privilege; inadequate protection of information can still demonstrate lack of confidentiality.[159] Because ECPA's privilege protection applies only to *otherwise* privileged communications, common law principles still control.[160]

No case law supports the idea that criminality of interception negates waiver. ECPA has not necessarily protected application of the privilege to cellular and cordless phones.[161] While its potential use to substantiate the privilege remains untested by the courts, the ECPA does not appear to demonstrate the necessary expectation of confidentiality to ensure the applicability of the privilege to Internet electronic mail.[162]

While ECPA prohibits interception, it does not necessarily deter hackers. It is hardly surprising that commentators have "found no cases saying reliance on federal law is sufficient to preserve the attorney-client privilege or confidentiality of hacked e-mail."[163]

> Assuming the privilege does apply to an e-mail message ..., it is clear that the privilege may nonetheless be lost under traditional rules of interpretation if the e-mail falls into the wrong hands. Professor Wigmore ... says:
>
> > All involuntary disclosures, in particular, through the loss or theft of documents from the attorney's possession, are not protected by the privilege on the principle that, since the law has granted secrecy so far as its own process goes, it leaves to the client and attorney to take

158. Georges, *supra* note 76, at 38.
159. *See* Connolly, *supra* note 22.
160. *See* Rose, *supra* note 11, at 211-12.
161. *See* text accompanying *infra* Part IV.C.2.b.
162. *See* Matthews, *supra* note 45, at 291-92.
163. Grant, *supra* note 114, at 33.

> measures of caution sufficient to prevent being overheard by third persons. The risk of insufficient precautions is upon the client.[164]

The privilege does not apply to all communications that should have been kept confidential; it only applies when confidentiality actually incurs. The relevant measure for actual confidentiality is the reasonable potential for interception by third parties, not those third parties' potential liability or the possibility that they will be deterred from interception thereby. In fact, it might be argued that there would be no need to make interception of electronic mail illegal were the threat of interception not substantive. That is, illegality might not imply infrequency, but frequency.

Those who promote the use of ECPA to ensure the privilege appear to either ignore or miscomprehend the primary argument against its use—namely, that if the communicating parties have subjective reason to believe that their means of communication is susceptible to interception, or if there is objective reason to believe the same, the privilege will not protect those communications. This misunderstanding may be illuminated through use of an admittedly extreme hypothetical. A lawyer and client who discuss private information over a telephone connection, which they know is wiretapped by an adverse party, will have no reasonable expectation of confidentiality. The privilege will not apply, despite the language of 18 U.S.C. § 2517(4). Once this baseline is established, it seems that the ECPA privilege proponents are attempting to argue matters of degree. Certainly, if the lawyer and client merely believe that the phone may be tapped, the privilege may or may not apply based on the common law principles of the privilege. Logically, this is the probable meaning of the phrase "otherwise privileged."

That attorney and client need not demonstrate reasonable belief that telephony is a generally secure means by which to communicate appears due to the technology of the medium and its history of supporting the privilege, not to § 2517(4). Indeed, the Safe Streets Act of 1968,[165] of which ECPA is a component, was enacted not to reduce the ability of a party to introduce intercepted conversations, but to enhance it. The year prior to its enactment, the Supreme Court had recognized a Fourth Amendment privacy interest in telephone conversations.[166] By setting out procedures to be followed for lawful wiretaps, the eavesdropping provi-

164. Smith, *supra* note 51.
165. 42 U.S.C. § 3711 (1976 & Supp. IV 1980).
166. *See* Katz v. United States, 389 U.S. 347 (1967).

sions that we now call ECPA were designed to make introduction of intercepted conversations constitutional.

C. Some Claim the Use of Unencrypted Internet E-mail Will Maintain the Privilege

"Because the use of e-mail has assumed such a prominent place in the business world, public policy strongly supports the extension of the attorney-client privilege to cover this means of communication."[167] That may well be true. However, some commentators have leapt from the proposition that electronic mail *should be availed* of the privilege, as a matter of policy, to the claim that it *is actually availed*, as a matter of law. Unfortunately, this laudable goal belies the truth—that unencrypted electronic mail sent over the Internet is in fact susceptible to interception, and that such interception may at least sometimes jeopardize the privilege.

1. Physical Security of Communications

Several commentators have made claims which are simply untrue, such as analogizing the difficulty of tapping a phone line to that of intercepting a TCP/IP[168] transmission. Some statements to this effect are thoroughly misinformed;[169] others merely mistake details.[170] These commentators believe that lack of physical network access[171] over the mandatory

167. Matthews, *supra* note 45, at 295.

168. TCP/IP (Transmission Control Protocol/Internet Protocol) is the standard set of protocols used on the Internet. It was "developed to allow cooperating computers to share resources across a network." Charles L. Hedrick, *What is TCP/IP?* (visited Dec. 2, 1999) <http://oac3.hsc.uth.tmc.edu/staff/snewton/tcp-tutorial/sec1.html>.

169. *See, e.g.*, Gidari, *supra* note 111, at 2 ("To intercept an Internet communication ... requires a wiretap. Thus, there is no greater insecurity when the Internet communication is in transit over the phone lines than there is with an ordinary phone.").

170. *See, e.g.*, Perritt *supra* note 129 ("If an intruder were on the same subnetwork as the law firm or its correspondent (or if she managed to get physical access to the relevant packet path), the physical access would exist, and all the intruder need do is program a computer to search for the packets with the desired addresses. If the intruder does not have access to those subnets, however, he must establish a physical connection to a wire or optical fiber over which the traffic moves. This is a significant barrier to eavesdropping not present when an intruder wishes to intercept cellular telephone messages. The main barrier to eavesdropping on email thus is equivalent to the principal barrier to eavesdropping on ordinary telephone conversations: effectuating a physical tap. On the other hand, once physical access is obtained, screening for the desired information is much easier in the case of Email because a computer can be programmed to do it, while a human being must screen voice conversations to find the desired one.").

171. That is, lack of a physical wiretap.

portions of the message's route, packetization,[172] and dynamic routing[173] over the remainder of its journey, make interception of Internet traffic difficult.[174] While it is theoretically possible that these limitations could themselves provide "reasonable precautions," there is a lack of case law to support such a claim.[175]

As a technical matter, moreover, physical access is not required, and the multiplicity of potential routes is not itself sufficient protection. While packetization and dynamic routing protect Internet traffic over most of its journey, the closer a potential interceptor can get to the points of origination and receipt, the more susceptible to eavesdropping a message becomes. Although a TCP/IP packet can take many different paths across the Internet between the same two nodes,[176] certain nodes are common to each potential route.[177] All told, many specific and identifiable nodes must typically be traversed by a message packet in order to be transmitted from sender to recipient.[178] Compromising any one of these nodes—gaining metaphysical access—enables access to the data stream without physical access to a vulnerable point on the network.

If there was a time when dynamic routing led to vastly different paths of travel for multiple packets in a single message, it is no longer. A sampling of routes between this author's home computer and three remote

---

172. Packetization is the process of dividing Internet communications into smaller pieces, or packets, for delivery.

173. Dynamic routing is the ad hoc direction of individual packets based on estimated efficiency of different network segments.

174. *See, e.g.*, Allison, *supra* note 122, at 18.

175. *See* Smith, *supra* note 51.

176. A node is any device connected to a network. I use the term to refer primarily to users' computers, servers, and routers, but other devices such as terminal servers and printers are nodes as well.

177. By way of analogy, my father can drive on any number of roads from his home to the grocery store, but his journey inevitably begins in his driveway and ends in their parking lot.

178. Typically including, in order of receipt, several of the following: (1) the sender's computer; (2) the sender's e-mail server; (3) the sender's e-mail server's SMTP gateway if one is used; (4) the router connecting the sender's local area network ("LAN") to the leased line to its Internet service provider ("ISP"); (5) the router connecting the leased line to the sender's ISP; (6) the router connecting the sender's ISP to the leased line to its backbone provider; (7) the router connecting the leased line to the sender's ISP's backbone; (8) the router connecting the leased line from the recipient's ISP to its backbone; (9) the router connecting the recipient's ISP to the leased line to its backbone provider; (10) the router connecting the leased line from the recipient's LAN to its ISP; (11) the router connecting the leased line to the recipient's LAN; (12) the recipient's e-mail server's SMTP gateway if one is used; the recipient's e-mail server; and finally, (13) the recipient's computer.

computers—<www.echonyc.com>, <echonyc.echonyc.com>, and <boalthall.berkeley.edu>—on six separate occasions during September and October 1999, reveals far less variation than would suffice to provide any real degree of protection.[179] All told, at least half of the individual routers traversed by transcontinental packets sent a month apart were identical. Compare packets sent a mere 24 hours from each other, and any variance is minor or nonexistent. Clearly, one can no longer expect that the path of multiple packets from the same electronic mail message will look like anything other than the trail of a brood of lemmings on its terminal stroll. Although it is doubtful that the variation described by technical protection proponents has existed during the past decade, one may presume that its remaining artifacts largely disappeared with the increasing professionalism of the Internet and the relative stability it entails. After all, from the outset, dynamic routing has had three primary goals: to reduce demands on the network, to increase the efficiency with which communications travel, and to route around unstable nodes. As the topology of the Internet has become more stable, the network environment changes less frequently, and there is comparatively little to be gained from updating router tables that have grown so enormous that updating them with the same frequency as a decade ago has become technically untenable.

Identifying necessary nodes for an Internet mail communication is thus no longer difficult. However, the mere ability to identify the path of travel is useless to a potential eavesdropper without the ability to intercept the packets on their path. Some 85% of Internet routers are manufactured by a single manufacturer.[180] That company promotes on the cover of its 1998 Annual Report that, "Virtually all of the information on the Internet travels across the systems of one company[:] Cisco Systems."[181] While this is positive for Cisco's market share, it may not be the best scenario for security. That all those routers are based on similar software and hardware means that they share common vulnerabilities; that they are so ubiquitous gives hackers both the incentive and the opportunity to learn as much as possible about those vulnerabilities. As a result, compromising one of those necessary nodes and thereby gaining metaphysical access is quite a bit more possible than would make for comfort.

---

179. Tables of these routes follow this Comment as Appendices. See *infra*, page 1160.

180. *See* Dean Takahashi, *Technology & Telecommunications: Cisco's Net for Quarter Surged 61% as Firm Continued to Dominate Market*, WALL ST. J., Feb. 5, 1997, at B2.

181. CISCO SYSTEMS, INC., 1998 ANNUAL REPORT, at front cover (1999) *available at* <http://www.cisco.com/warp/public/749/ar98/pdf/ar98.pdf> (PDF file).

2. *Insecurity of Other Media*

Often, those who accept that the Internet is vulnerable, yet claim that the attorney-client privilege applies to electronic mail, feel that demonstrating the lack of safety in other media will bolster their argument. This reasoning by analogy tends to fall short of conclusive proof, in part because the case law surrounding wired and wireless telephony is not uniform, but can only be understood on a case-by-case basis. In fact, it was only thirty years ago—nearly a century after Alexander Graham Bell's most famous invention—that the Supreme Court first recognized any reasonable expectation of privacy in any telephone conversations.[182]

On the whole, these advocates have a point, in that the differences are largely of degree.

> The problem is that security—on the Internet—is singled out as deserving special attention, while similar risks with other forms of communication are simply ignored.... [O]ther technologies—cellular phones, regular phones, voice mail, faxing, (even couriers)—have their own set of risks. But when the Internet is discussed in isolation from the alternatives, it's difficult to judge the *comparative* risks.[183]

Absolute security is not attainable in any medium; neither is it required to maintain the privilege.[184] Instead, "courts focus both on the precautions taken to preserve the confidentiality, and on the parties' reasonable expectation of privacy."[185] Examples of communication vulnerabilities include intentional or inadvertent interception of telephone or face-to-face conversation, misdirection or insecure storage of mail or faxes, lip-reading, and the compromise of persons with pertinent knowledge.[186]

Perhaps because telephone conversations are almost uniformly found to maintain the privilege, their putative insecurity is widely hyped by proponents of affording the same status to unencrypted electronic mail. Admittedly, telephone calls can be tapped more easily than most people think. Printed materials provide instructions on so doing, and additional technical expertise can be easily had from disgruntled technical workers among "the thousands of recently 'downsized' telephone company em-

---

182. *See* Matthews, *supra* note 45, at 273 (citing Katz v. United States, 389 U.S. 347, 360 (1967)).

183. Allison, *supra* note 122, at 16 (emphasis in original).

184. *See* Leibowitz, *supra* note 17.

185. *Id.*

186. *See, e.g.*, *id.*; Freivogel, *supra* note 26.

ployees."[187] Yet no court or ethics committee requires use of a secure wired telephone to demonstrate a justifiable expectation of confidentiality.[188]

But it is an insupportable leap from the fact that wired telephony is not perfectly secure to the claim that "[a]s a practical matter, it is far more difficult to access e-mail sent through the Internet than it is to tap a telephone line or to snatch a letter from a mailbox."[189] With both the mails and telephony, a potential interceptor must actually gain physical access to the medium. In contrast, a hacker need merely compromise a node on the network which is necessary to a transmission between attorney and client, and such access need not be physical.[190]

The analogies to wireless phones are more clearly damaging to protection of electronic mail. Despite protection afforded to "wireless communications" under ECPA, courts have found that cellular and cordless phones lack sufficient confidentiality to support the privilege.[191] In *Tyler v. Berodt*, the Eighth Circuit found a lack of confidentiality in use of cordless phones, but *Tyler* was decided before cordless phone eavesdropping was made illegal in 1994.[192] That statutory change, however, has not had the expected effect on the outcome of cases. Recently, courts have held that one party's use of a cordless phone, even without the other party's knowledge, defeats the expectation of privacy held by either.[193]

"Even though it is a federal crime to intercept [cellular phone] communications, the ease with which such communications can be intercepted apparently led [several state and local bar associations] to the conclusion that such communications are not 'made in confidence' and therefore could not fall within the privilege."[194] Although no courts have apparently ruled on application of the privilege to cell phones, relying on it "would be foolhardy."[195]

---

187. *See, e.g.*, Freivogel, *supra* note 26.

188. *See id.*

189. Pope & Pope, *supra* note 53, at 142.

190. *See supra* Part IV.C.1.

191. *See* Matthews, *supra* note 45, at 293 (citing Tyler v. Berodt, 877 F.2d 705, 706-07 (8th Cir. 1989); People v. Fata, 529 N.Y.S.2d 683, 696 (Rockland County Ct. 1988); State v. Smith, 438 N.W.2d 571, 577 (Wis. 1989)).

192. *See* Rogers, *supra* note 25, at 61.

193. *See* Matthews, *supra* note 45, at 293 (citing McKamey v. Roach, 55 F.3d 1236, 1240 (6th Cir. 1995); *In re* Askin, 47 F.3d 100, 104-06 (4th Cir.), *cert. denied*, 516 U.S. 944 (1995)).

194. Smith, *supra* note 51.

195. *Id.*

At the risk of sinking into the analogical muck, the modern computer network tends to look less like wireline telephony than like wireless. Wireline telephony is circuit switched; that is, an exclusive connection is established between two points, and communications travel through that connection. With wireless communications, by contrast, the recipient must merely know the frequency upon which the communication is to be transmitted. With cellular or cordless phones, all that maintains privacy is that no one else happens to be listening to that particular frequency in that particular location at that particular time. Similarly, Ethernet networks broadcast the same information across the entirety of their unrouted network; whether a machine "hears" a packet going by depends on whether it opts to or not. Most of the time, computers are configured to ignore all packets not intended for them, but reprogramming them to do otherwise is relatively trivial.[196]

Furthermore, electronic mail invokes additional security concerns compared to telephone calls and voice mail.[197] In general, no record is made of the content of phone calls, although transactional data are maintained.[198] Voice mail, while also stored until listened to and deleted, is usually disposed of earlier than electronic mail. Furthermore, it is usually not backed up to protect against system failure, as are most e-mail servers, and voice mail systems usually delete messages after a certain time in order to recover storage space. Nor is the content of either telephone calls or voice mail easily searched.

Some firms use e-mail disclaimers like those on fax cover sheets; such disclaimers might demonstrate intent to maintain confidentiality, limit improper distribution, and bind lawyers who accidentally receive to protect the privilege.[199] But since interception is already a felony, a paragraph of legalese is unlikely to dissuade many.[200] In fact, use of disclaimers may imply belief that e-mail is insecure.[201]

---

196. This is commonly known as "packet sniffing," and is discussed in detail in *infra* Part IV.D.2.e.

197. *See, e.g.*, Allison, *supra* note 122, at 16-20.

198. Transactional data recorded tend to be that required for billing and system monitoring purposes, including the fact that a call was made by a specific party to another party, the time of the call, and its duration.

199. *See* Rogers, *supra* note 25, at 66.

200. *See id.*

201. *See id.*

D. Some Claim the Use of Unencrypted Internet E-mail Will Threaten the Privilege

As new technologies help provide greater security to communications, mechanisms by which that security can be breached tend to develop apace.[202] Electronic mail is no exception. This has significant implications for the privilege, since at its root, "the availability of a claim of privilege to protect an e-mail communication turns on whether a court can be persuaded that the risk of meaningful interception is so trivial that the communication can be deemed to have been 'made in confidence.'"[203]

Those who doubt the security of electronic mail transmitted over the Internet are no less prone to hyperbole than their opponents. One extreme perspective is that "the ease with which electronic mail messages can be intercepted by third parties means that communicating by public electronic mail systems, like the Internet, is becoming almost as insecure as talking in a crowded restaurant."[204] Technologists, too, can be bitten by the overstatement bug. "E-mail security is in a perilous state. A closed user domain can be adequately secured, but what happens when messages cross organizational boundaries?"[205]

Explanations for why threats to Internet security, while serious, have been exaggerated tend to hinge on phenomena of information distribution combined with inconsistent case law surrounding the privilege. Allison discusses what he calls the "airplane magazine effect"—when "Someone Way High Up In The Food Chain" reads an oversimplified description of a technical problem and decides they have to fix it.[206] Internet issues are particularly susceptible to this type of superficial treatment because the technology is poorly understood by editors and readers, and a few horror stories can be used to justify maintenance of the status quo.[207] "And to be fair, in the context of attorney-client communications, even the *prospect* of poor security warrants serious attention."[208]

Increased awareness of the risks of Internet e-mail have resulted in such steps as increased use of disclaimers and legislation like New York State Civil Practice Law and Rules § 4548.[209] "One thing is clear: almost

---

202. *See* Lapidus, *supra* note 73, at 39 (citing Arizona Ethics Op. No. 95-11 (1995); Association B. City N.Y. Comm. Prof. Jud. Eth., Formal Op. No. 1994-11 (1994)).

203. Smith, *supra* note 51.

204. Froomkin, *supra* note 93, at 724.

205. Willis, *supra* note 114, at 108.

206. Allison, *supra* note 122, at 16.

207. *See id.*

208. *Id.*

209. *See* Lewis, *supra* note 124.

everyone seems to perceive that the Internet is less secure than the traditional mail system and the telephone networks."[210] These fears are well-supported—there are legitimate reasons to worry about security of computer files generally, and electronic mail in particular.[211] In fact, the threat of infiltration of computer records may exceed that of paper files, even with individual login names and passwords.[212]

1. *Security of Computer Data in General*

Many of the security problems associated with unencrypted electronic mail are not unique to such transmissions, but are endemic to computer data generally, whether or not the computer in question is even networked.

Employers and MIS staff have high levels of access to data. The very technology of computer networks centralizes information access. Usually, this is one of the primary benefits of computerization, but it also provides an unprecedented ability to review that information without requiring physical access to those with technical or managerial needs or desires for such access—including MIS staff and employers.[213] Furthermore, electronic data may be searched easily using sophisticated techniques that are likely to pinpoint useful information. Since e-mail is usually sent in readable text format, automated analysis thereof tends to be particularly fruitful.[214] Finally, computer files are difficult to delete and backups tend to persist even after the original files are long gone.[215]

2. *Security of Computer Networks and Internetworks*

The Simple Mail Transfer Protocol ("SMTP") and most other mail protocols in use were designed to maximize the likelihood that a message will be received, not that its contents will be kept confidential. "You need only watch the typical SMTP gateway to understand how lax intercompany e-mail security is. Messages often pass in the clear, and undeliverable messages are dumped at the gateway or in a postmaster mailbox. It's a sight most e-mail administrators would rather keep hidden."[216]

"Encryption services are not normally in place for ... SMTP links" which transfer e-mail between the in-house system and the Internet.[217] A gateway, as these electronic links between the firm and the outside world

---

210. Flaming, *supra* note 13, at 183.
211. *See generally* Rose, *supra* note 11 at 202-05.
212. *See* Traynor, *supra* note 81.
213. *See* Rose, *supra* note 11, at 202-05.
214. *See* Matthews, *supra* note 45, at 279.
215. *See supra* Part III.A.2.
216. Willis, *supra* note 114, at 108.
217. *Id.*

are known, might conceivably provide enhanced security, but those in use today unwarrantedly fail to verify the identity of client systems, give too much control and oversight to the network administrator, and are too blunt a weapon against intrusion to truly be effective.[218] Furthermore, even encrypted mail must necessarily use unencrypted addressing schemes. While the generated data are merely transactional, not content-based, knowing who has talked to whom may lead to further discoveries.[219]

ISP staff have physical access to any transmission between a local-area network ("LAN") and any other node on the Internet.[220] ISP and MIS personnel will necessarily have access to information in and on its way to user accounts, whether they avail themselves of it or not.[221] Furthermore, ISP end-user agreements are more frequently requiring permission to divulge contents to third parties.[222]

Computer files may be duplicated and transferred more easily than paper. "Electronically stored records are far more portable and accessible than paper records. An individual electronic file may be found on one ... or on several personal computers ... or ... disks. If a party is 'networked,' ... then the number of people who can access the electronic file or the number of copies that could exist is expansive."[223]

Node impersonation, or "spoofing," is telling a computer to pretend to be another computer.[224] A "spoofed" node can pretend to be necessary to a potentially privileged transmission. The risk to e-mail from spoofing is relatively low, given the use of servers and routers to transfer information without user intervention, but it is present.[225] Probably the devices at greatest risk for spoofing are routers, in that they are mere milestones on the path of a packet. Copies of mail and other Internet traffic can be siphoned off by a spoofing router without any realistic chance of detection.

A node which has been programmed to "sniff" packets can provide access to inappropriate information. Sniffing is telling a computer not to ignore packets intended for other computers.[226] Some proponents of applying the privilege overstate the difficulty of intercepting Internet traffic;[227]

---

218. *See id.*
219. *See* Matthews, *supra* note 45, at 279.
220. *See* Rose, *supra* note 11, at 202-05.
221. *See* Allison, *supra* note 122, at 18.
222. *See* Lewis, *supra* note 124.
223. Silvernail, *supra* note 61, at 180.
224. *See* Flaming, *supra* note 13, at 184.
225. *See id.*
226. *See id.* at 183-84.
227. *See* Freivogel, *supra* note 26.

in fact, spoofing does not require hardware or luck. While Freivogel is correct to disparage the oft-invoked "postcard" analogy for e-mail, neither is "[a]n Internet message ... like a metal box with a lock that few criminals are competent to pick."[228] Freely-available, intuitive, and inexpensive software will capture all network traffic passing by, including most electronic mail account passwords.

Sniffers are frequently used by network technicians to pinpoint the source of network failures. For instance, in attempting to determine whether a specific node was generating any Ethernet traffic whatsoever, or was instead silent, this author once used a sniffer to capture all network traffic on a client's LAN for fifteen seconds. Coincidentally, the president of the company chose that moment to check his electronic mail. As one might imagine, revelation of his password was a catalyst for institution of additional security measures.

Interception software positioned at an appropriate location—namely, on or near the respective networks of attorney and client—can compromise either individual messages or entire accounts, or both. And like any other software, it can be placed and run on an inadequately-secured machine without its owner's or operator's knowledge. Most dangerous of all, sophisticated sniffers can target traffic according to certain criteria, such as the addresses of the originating and destination nodes, and the type of traffic.[229] Thus, a sniffer placed at a necessary node between attorney and client can be configured to capture all SMTP traffic between the organizations' e-mail servers for later analysis.

V. PRACTICAL ADVICE FOR THE PRUDENT PRACTITIONER

To date, no case has held a lawyer liable for breach of the privilege or for the related ethical duty of confidentiality based on use of electronic mail.[230] Unencrypted e-mail may well be sufficiently unlikely to be intercepted that it can probably be used for the "vast majority of messages most attorneys will send or receive."[231] While technical and legal standards concerning encryption evolve, however, practitioners must choose

228. *Id.*

229. Most sniffers are able to target specific traffic by the "port" number used therefor. There are over 65,000 available ports; however, both machines must agree on the port to use. Therefore, traffic which commonly travels between networks, such as SMTP and HTTP, uses default ports to allow intercommunication.

230. *See, e.g.*, Freivogel, *supra* note 26.

231. Lapidus, *supra* note 73, at 42.

between two starkly divergent perspectives on prescribing policies governing communication with clients by electronic mail.

Ethics boards of various states, and now the ABA, have joined commentators in insisting that any concerns over the confidentiality of Internet electronic mail are farfetched. Unfortunately, their analyses are invariably flawed by both ignorance of Internet and encryption technologies and by their misunderstanding of the legal standards for attorney-client privilege. Moreover, these shortcomings are compounded by their proponents' self-interest in ensuring that the umbrella of privilege extends as widely as possible. Yet the champions of unquestioned privilege over Internet electronic mail appear to have momentum on their side. Since the hallmark of protected communications is reasonable belief in rather than actual confidentiality, this growing chorus of voices may suffice to ensure that a court faced with these issues will find that electronic mail supports privilege without any consideration to technological or legal context. Thus, the prospect of finding safety in numbers by relying on the ECPA tautology and pronouncements of ethics boards is tempting indeed.

On the other hand, a practitioner would be more prudent to seek a different kind of safety in numbers—that is, in the algorithms that form the basis for modern cryptography. No commentator or ethics board has questioned that encrypted Internet electronic mail supports the privilege. Indeed, it appears universally-accepted that cryptography makes such messages at least as safe as other media known to protect their contents. The very volume of pronouncements on the issue should give the reader pause: if application of the privilege to unencrypted electronic mail were as clear as some suggest, there would be no need to discuss it at all.

Clearly, the practical use of encryption will continue to become easier, while the potential bounty awaiting the interceptor of electronic mail sent over the Internet will continue to multiply.[232] These trends make the possibility that a court will eventually find negligence in the failure to encrypt increasingly likely and, arguably, inevitable. Because there is a first time for everything, this comment concludes with tips for attorneys and their clients who wish to avoid the difficulties which inhere in becoming a test case.

232. While determining the probability of interception will remain impossible as a practical matter, *see* Jones, *supra* note 77, there is no reason to believe that it will not stay relatively constant. *See also* Lapidus, *supra* note 73, at 42.

A. Don't Rely on the ECPA

It is reasonable to note that "no communication is secure if someone is willing to violate criminal laws to get the information,"[233] because every security measure can be overcome, at least in theory. Indeed, the fact that interception of an electronic mail message is a federal felony will probably deter many potential interceptors.[234] Nonetheless, a prudent attorney probably will not wish to rely on the rationality of potential criminals to ensure applicability of the attorney-client privilege to her communications. Until a court has held that the mere criminality of interception suffices to maintain privilege, reliance on ECPA and analogous statutes seems inadvisable.

B. Address Electronic Security as an Integral Aspect of an Overall Security Strategy

1. Conduct a Confidentiality Audit

Chances are high that communications security holes exist in both law firms' and their clients' offices. Faxes containing confidential information are often left waiting at facsimile machines after being sent or received. The weaknesses of popular voice mail systems and private branch exchanges ("PBXs") are well-known and exploitable. Concerns about Internet security should be a catalyst for overall examination, not a palliative to convince either the attorney or the client that all is clear.

2. Involve MIS Staff in the Review

MIS staff learn early on that when they have a choice, they should maximize safeguards against loss of data. Users accidentally delete or modify important computer files on a frighteningly frequent basis. The ability to recover information feared lost is a magic trick that has won many friends, and probably not a few promotions. So long as adequate storage space is available, MIS rarely sees a downside to maximum preservation; as a result, files may be maintained longer than necessary for internal needs.[235]

---

233. Freivogel, *supra* note 26.

234. *See id.*

235. For example, network operating systems often have settings for the preferred and minimum amount of time to wait before forgetting the location of a file which has been deleted and permit specification of directories whose contents are immediately purged if deleted. Electronic mail software often supports filtering, which can be customized to delete mail according to criteria such as date sent.

An MIS department which is educated about privilege and discovery concerns will be able to make informed decisions about optimizing security settings on a server. With data-protection measures such as backup strategies, even minor modifications—for instance, the order in which specific directories containing files of varying vulnerability are written to tape[236]—can have major effects.

3. *Include Electronic Documents in Retention Policies*

Despite the clear threat, document retention policies almost always cover paper documents, but not electronic ones.[237] The searchability and persistence of electronic data make them more vulnerable to damaging discovery than other documents. If your or your clients' document retention policies have not yet caught up with new technology, this would be an opportune time to update them. If no formal policies exist, develop them and be sure to include computer data. As with any document retention policy, care must be taken to avoid spoliation, the unethical and potentially illegal destruction of evidence. However, remember to treat computer files as you would paper ones; standards developed in other media should be brought into the electronic realm.

4. *Use Contracts to Bind Employees and Contractors to Maintain Confidentiality*

The privilege can protect communications by nonlawyers with access to sensitive legal material. All employees, as well as outside support personnel with access to sensitive information, such as ISP staff and computer consultants, should be made to sign promises to maintain confidentiality. Even if these contracts may be found ineffective to support the privilege's confidentiality and non-waiver requirements without additional measures, their use may evince subjective intent to maintain confidentiality and may help educate their signatories about security concerns.

C. Encrypt Sensitive Materials and Communications

The problems with implementing a firm-wide encryption strategy should not dissuade users from encrypting sensitive materials when appropriate. Even the built-in encryption offered by contemporary word processing software can provide greater security than cleartext transmis-

236. A directory written to the beginning of a tape will be erased each time the tape is reused; one written to its end may be recoverable even after subsequent backups. Thus, if a daily backup run includes both privileged information like client files and unprivileged information like backups of software applications, backing up the privileged data first ensures that reuse of the tape will destroy it, even if multiple copies of software remain.

237. *See* Lovell & Holmes, *supra* note 82, at 8.

sion or storage, and may help prove subjective intent to keep the specific communication secret. The password to the file will need to be told by sender to recipient in a separate telephone call and recorded for future access. This makes the process cumbersome compared to a fully-implemented public-key infrastructure, but its use may make the difference between privilege and its absence.

Strong encryption mechanisms are becoming easier to use and implement. If a client wishes to use electronic mail frequently for attorney-client communications, discuss the benefits of implementing a public-key cryptosystem, and develop a strategy to ensure its use. If and when you start to use encryption, be sure to follow through. Against a background policy requiring its use, a court might find lack of confidentiality or constructive waiver in failure to encrypt a specific communication.

Encryption cannot solve every security problem. Low-technology means of access to computer information—physical compromise of a user's password or computer, for instance—will still leave information vulnerable.[238] Yet when used properly, the best encryption makes electronic mail at least as safe as any other extant medium. As encryption becomes easier and more effective to use and implement, its use will probably become a standard aspect of business communications generally, and legal practice specifically.

238. *See* Jones, *supra* note 77.

Appendix 1. Traceroute Results, 24.142.58.224 to <www.columbia.edu>

Date/Time	*Step 1*	*Step 2*	*Step 3*	*Step 4*	*Step 5*	*Step 6*
9/18/99, 11:25 pm	**24.142.50.1**	**208.166.60.2**	**166.48.15.249**	**204.70.4.81**	**206.157.77.66**	**144.232.4.33**
9/20/99, 9:48 pm	**24.142.50.1**	**208.166.60.2**	**166.48.15.249**	**204.70.4.81**	**206.157.77.66**	**144.232.4.33**
10/12/99, 10:08 pm	**24.142.50.1**	**208.166.60.2**	**166.48.15.249**	**204.70.4.81**	**206.157.77.66**	**144.232.4.33**
10/13/99, 9:46 pm	**24.142.50.1**	**208.166.60.2**	**166.48.15.249**	**204.70.4.81**	**206.157.77.66**	**144.232.4.33**
10/16/99, 1:49 pm	**24.142.50.1**	**208.166.60.2**	**166.48.15.249**	**204.70.4.81**	**206.157.77.66**	**144.232.4.33**
10/17/99, 9:36 pm	**24.142.50.1**	**208.166.60.2**	**166.48.15.249**	**204.70.4.81**	**206.157.77.66**	**144.232.4.33**

Step 7	*Step 8*	*Step 9*	*Step 10*	*Step 11*	*Step 12*	*Destination*
n/a	144.232.5.110	169.130.1.126	169.130.2.21	**169.130.12.6**	**128.59.247.3**	**128.59.35.36**
n/a	144.232.5.110	169.130.1.102	169.130.2.21	**169.130.12.6**	**128.59.247.3**	**128.59.35.36**
144.232.8.177	169.130.1.25	*169.130.2.70*	*169.130.12.13*	**169.130.12.6**	**128.59.1.5**	**128.59.35.17**
144.232.8.177	169.130.1.33	*169.130.2.70*	*169.130.12.13*	**169.130.12.6**	**128.59.1.5**	**128.59.35.17**
144.232.8.177	169.130.1.33	*169.130.2.70*	*169.130.12.13*	**169.130.12.6**	**128.59.1.5**	**128.59.35.17**
144.232.8.177	169.130.1.33	*169.130.2.70*	*169.130.12.13*	**169.130.12.6**	**128.59.1.5**	**128.59.35.17**

Legend: **bold** = included in all routes ***bold italic*** = included in all but one route *italic* = included in all but two routes

Appendix 2. Traceroute Results, 24.142.58.224 to <echonyc.echonyc.com>

Date/Time	*Step 1*	*Step 2*	*Step 3*	*Step 4*	*Step 5*	*Step 6*
9/18/99, 11:28 pm	**24.142.50.1**	**208.166.60.2**	**166.48.15.249**	**204.70.9.41**	***204.70.10.158***	146.188.148.218
9/20/99, 9:50 pm	**24.142.50.1**	**208.166.60.2**	**166.48.15.249**	**204.70.9.41**	204.70.10.162	146.188.148.214
10/12/99, 10:11 pm	**24.142.50.1**	**208.166.60.2**	**166.48.15.249**	**204.70.9.41**	***204.70.10.158***	146.188.148.210
10/13/99, 9:47 pm	**24.142.50.1**	**208.166.60.2**	**166.48.15.249**	**204.70.9.41**	***204.70.10.158***	146.188.148.214
10/16/99, 1:50 pm	**24.142.50.1**	**208.166.60.2**	**166.48.15.249**	**204.70.9.41**	***204.70.10.158***	146.188.148.210
10/17/99, 9:38 pm	**24.142.50.1**	**208.166.60.2**	**166.48.15.249**	**204.70.9.41**	***204.10.10.158***	146.188.148.210

Step 7	*Step 8*	*Step 9*	*Step 10*	*Step 11*	*Destination*
152.63.48.234	152.63.3.153	146.188.178.209	*146.188.177.113*	**198.67.15.1**	**198.67.15.2**
152.63.49.50	152.63.3.201	146.188.178.193	146.188.177.125	**198.67.15.1**	**198.67.15.2**
152.63.48.238	152.63.3.149	146.188.178.177	*146.188.177.113*	**198.67.15.1**	**198.67.15.2**
152.63.49.42	152.63.3.201	146.188.178.197	146.188.177.125	**198.67.15.1**	**198.67.15.2**
152.63.48.238	152.63.3.149	146.188.178.177	*146.188.177.113*	**198.67.15.1**	**198.67.15.2**
152.63.48.238	152.63.3.149	146.188.178.177	*146.188.177.113*	**198.67.15.1**	**198.67.15.2**

Legend: **bold** = included in all routes ***bold italic*** = included in all but one route *italic* = included in all but two routes

Appendix 3. Traceroute Results, 24.142.58.224 to <boalthall.berkeley.edu>

Date/Time	*Step 1*	*Step 2*	*Step 3*	*Step 4*	*Step 5*
9/18/99, 11:31 pm	**24.142.50.1**	**208.166.60.2**	**166.48.15.249**	204.70.4.89	209.185.9.9
9/20/99, 9:50 pm	**24.142.50.1**	**208.166.60.2**	**166.48.15.249**	204.70.4.89	209.185.9.9
10/12/99, 10:13 pm	**24.142.50.1**	**208.166.60.2**	**166.48.15.249**	204.70.4.93	209.185.9.13
10/13/99, 9:47 pm	**24.142.50.1**	**208.166.60.2**	**166.48.15.249**	204.70.4.93	209.185.9.13
10/16/99, 1:51 pm	**24.142.50.1**	**208.166.60.2**	**166.48.15.249**	204.70.4.93	209.185.9.13
10/17/99, 9:39 pm	**24.142.50.1**	**208.166.60.2**	**166.48.15.249**	204.70.9.131	206.24.210.61

Step 6	*Step 7*	*Step 8*	*Step 9*	*Step 10*	*Step 11*
216.32.132.85	216.33.154.131	209.185.249.109	209.1.169.42	209.185.255.125	***209.185.111.30***
216.32.132.77	216.33.154.131	209.185.249.109	216.33.147.81	*216.33.147.163*	***209.185.111.30***
216.3.64.170	216.33.153.1	209.185.249.141	216.33.147.34	*216.33.147.163*	***209.185.111.30***
216.33.64.170	216.33.153.1	209.185.249.141	216.33.147.34	*216.33.147.163*	***209.185.111.30***
216.33.64.170	216.33.153.65	209.185.249.141	216.33.147.34	*216.33.147.163*	***209.185.111.30***
206.24.211.134	198.32.249.69	128.32.0.89	128.32.0.78	128.32.0.99	n/a

Step 12	*Step 13*	*Step 14*	*Step 15*	*Destination*
192.35.216.57	***198.128.16.21***	**128.32.2.1**	**128.32.235.100**	**128.32.25.39**
192.35.216.57	***198.128.16.21***	**128.32.2.1**	**128.32.235.100**	**128.32.25.39**
192.35.216.57	***198.128.16.21***	**128.32.2.1**	**128.32.235.100**	**128.32.25.39**
192.35.216.57	***198.128.16.21***	**128.32.2.1**	**128.32.235.100**	**128.32.25.39**
192.35.216.57	***198.128.16.21***	**128.32.2.1**	**128.32.235.100**	**128.32.25.39**
n/a	n/a	**128.32.2.1**	**128.32.235.100**	**128.32.25.39**

Legend: **bold** = included in all routes ***bold italic*** = included in all but one route *italic* = included in all but two routes