Journal of Technology Law & Policy

Volume 10 | Issue 2 Article 4

December 2005

Lawyers Still Worry too Much About Transmitting E-Mail Over the Internet

David Hricik

Amy Falkingham

SYMPOSIUM ARTICLES

LAWYERS STILL WORRY TOO MUCH ABOUT TRANSMITTING E-MAIL OVER THE INTERNET

David Hricik[*] *& Amy Falkingham*[**]

I. INTRODUCTION 266

II. ETHICAL OBLIGATIONS CONCERNING CLIENT CONFIDENCES 267

III. THE NATURE OF DUTY OF CARE 268

IV. THE LIKELIHOOD OF EAVESDROPPING DEPENDS ON HOW E-MAIL IS SENT 270
A. *Local Area Network Communications* 270
1. The Risk of Eavesdropping 270
2. Legal Protections 270
3. Ethics Authorities 271
B. *Direct Computer-Computer Transmissions* 272
1. The Risk of Eavesdropping 272
2. Legal Protections 273
3. Ethical Authorities 273
C. *Internet Communications* 273
D. *Virtual Private Networks or SSL Communications* 279
1. The Risk of Eavesdropping 279
2. The Legal Protections 280
3. The Ethical Authorities 280
E. *Password-Protected Communications Sent Outside the LAN, and with SSL or VPN Systems, Then Within One On-Line Service Provider* 281
1. The Risk of Eavesdropping 281
2. The Legal Protections 282
3. The Ethical Authorities 285

---

* David Hricik is an Associate Professor at Mercer University School of Law in Macon, Georgia.

** Amy Falkingham is a third year student at Mercer University School of Law.

V. E-MAIL SENT OVER THE INTERNET WITHOUT SSL OR VPN CONNECTIONS 287
A. *Encrypted Internet E-Mail* 287
1. The Risk of Eavesdropping 287
2. The Legal Protections 288
3. The Ethical Authorities 288
B. *Unencrypted E-Mail* 288
1. The Risk of Eavesdropping 288
2. The Legal Protections 291
3. The Ethical Authorities 292
a. The Early Opinions 292
b. The State of the Law Today 296

VI. CONCLUSION: LAWYERS STILL WORRY TOO MUCH 299

I. INTRODUCTION

Although in many ways technology has made the practice of law easier, the vast increases in storage capacity, the lightning-quick speed of communication, and the ability to transmit data over the Internet have made it more important for lawyers to consider the impact of technology on the core ethical issue of confidentiality. Digitalization of the practice of law means that a breach of a duty of confidentiality can have far greater consequences because greater amounts of information can be transmitted at lightning speeds. Where once it would have taken a truck and an army of burglars to steal an important but voluminous file, today that information can be attached to a single e-mail. The ethical duty remains the same, but the consequences differ and the precise acts needed to protect client confidentially involve the use of new technology and uncertain or even unknown risks.

This Article describes how lawyers can meet their obligation of confidentiality when dealing with e-mail transmission.[1] It updates articles written by David Hricik more than six years ago[2] — eons in the Internet

---

1. There are many other issues that the use of e-mail create. For example, it may be necessary to delete e-mail on an ISP in order to ensure that the e-mail remains within the scope of the federal wiretap statutes. *See generally* Daniel J. Solove, *Data Privacy and the Vanishing Fourth Amendment*, 29 CHAMPION 20 (May 2005) (explaining that the Department of Justice believes that read, but not deleted, e-mails are exempt from those laws).

2. *See* David Hricik, *Confidentiality & Privilege in High-Tech Communications*, 60 TEX. BUS. J. 104 (1997); *Lawyers Worry Too Much About Transmitting Client Confidences by Internet E-Mail*, 11 GEO. J. LEGAL ETHICS 459 (1998).

age — that became widely cited in support of the proposition that e-mail was secure for purposes of attorney-client communications.[3] Since those articles were published, a few authors have agreed with his conclusions,[4] while others have not.[5] Indeed, a very recent piece notes that the foundation for the conclusion that e-mail was safe to use has been called into question by a subsequent First Circuit decision.[6] In a rather Quixotic fashion, this Article presents a very careful inquiry into the factual risks and an analysis of the legal protections associated with e-mail, with the hope of ending this debate.

II. ETHICAL OBLIGATIONS CONCERNING CLIENT CONFIDENCES

There are two forms of inadvertent e-mail transmission. One occurs when a lawyer inadvertently includes as a recipient an unintended name.[7] The availability of xerography and proliferation of facsimile machines and electronic mail make it more likely that through inadvertence, privileged or confidential materials will be sent to opposing counsel by no more than the pushing of the wrong speed dial number on a facsimile machine.[8] Lawyers must take reasonable precautions to prevent inadvertent

---

3. *See, e.g.*, ABA Comm. on Ethics and Prof'l Responsibility Formal Op. 99-413 (1999); Sup. Ct. Ohio Bd. Comm'rs. on Grievances & Discipline OH Adv. Op. 99-2 (1999); Pa. B. Ass'n. Comm. on Legal Ethics & Prof'l Resp. Informal Op. No. 97-130 (1997); Ill. St. B. Ass'n. Advisory Op. on Prof'l Conduct No. 96-10 (1997).

4. *See, e.g.*, Sean M. O'Brien, *Extending the Attorney-Client Privilege: Do Internet E-mail Communications Warrant a Reasonable Expectation of Privacy?*, 4 SUFFOLK J. TRIAL & APP. ADVOC. 187 (1999).

5. *See, e.g.*, Micalyn S. Harris, *E-Mail Privacy: An Oxymoron*, 78 NEB. L. REV. 386 (1999).

6. *See* Yvette Joy Liebesman, *The Potential Effects of* United States v. Councilman *on the Confidentiality of Attorney-Client E-mail Communications*, 18 GEO. J. LEGAL ETHICS 893 (2005). *Infra* text accompanying notes 107-12.

7. The ABA recently mentioned inadvertent transmission of e-mail when analyzing waiver of privilege over a misdirected fax: "the availability of xerography and proliferation of facsimile machines and electronic mail make it technologically ever more likely that through inadvertence, privileged or confidential materials will be produced to opposing counsel by no more than the pushing of the wrong speed dial number on a facsimile machine." ABA Comm. on Ethics and Prof'l Responsibility Formal Op. 92-368 (1992). *Accord* Fla. St. Bar Assn. Comm. on Prof'l Ethics Op. 93-3 (1994) (stating that "Such an inadvertent disclosure might occur as part of a document production, a misdirected facsimile or electronic mail transmission, a 'switched envelope' mailing, or misunderstood distribution list instructions.").

8. ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 92-368 (1992). *Accord* Fla. St. Bar. Assn. Comm. on Prof'l Ethics Op. 93-3 (1994) ("Such an inadvertent disclosure might occur as part of a document production, a misdirected facsimile or electronic mail transmission, a "switched envelope" mailing, or misunderstood distribution list instructions.").

transmission of confidential information to third parties, and especially opposing counsel.[9] For example, some firms have policies that prohibit lawyers and staff from having opposing counsels' fax numbers or e-mail addresses stored in any automatically accessible way (such as in an address book on a mail program or a speed dial button on a fax machine). Inadvertent disclosure of privileged information can waive the privilege, or if not, it can let the cat out of the bag.[10] However, that aspect is not the focus of this Article.

The second common form of inadvertent transmission occurs when the message is sent only to its intended recipients, but it is sent in a way that permits third parties to review — that is, electronically eavesdrop on — the information. Depending on the technology, e-mail can create the risk of eavesdropping. This circumstance is the focus of this Article.

III. THE NATURE OF DUTY OF CARE

Most states have rules based on ABA Model Rule 1.6, which requires lawyers to maintain all information relating to the representation of a client in confidence, with narrow exceptions.[11] This aspect of the duty of

---

9. MODEL RULES OF PROF'L CONDUCT R. 1.6, cmt. 17 (2003) ("When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients.").

10. *See In re* Sealed Case, 877 F.2d 976 (D.C. Cir. 1989) (inadvertently disclosing privileged information waives the privilege); *but see* Georgetown Manor v. Ethan Allen Corp., 753 F. Supp. 936 (S.D. Fla. 1991) (inadvertent disclosure can never waive privilege); *see also* Alldread v. City of Grenada, 988 F.2d 1425 (5th Cir. 1993) (inadvertent disclosure can sometimes waive privilege).

11. As recently amended by the ABA, Model Rule 1.6 provides in full:

> (a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).
>
> (b) A lawyer may reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary:
>
> (1) to prevent reasonably certain death or substantial bodily harm;
>
> (2) to prevent the client from committing a crime or fraud that is reasonably certain to result in substantial injury to the financial interests or property of another and in furtherance of which the client has used or is using the lawyer's services;
>
> (3) to prevent, mitigate or rectify substantial injury to the financial interests or property of another that is reasonably certain to result or has resulted from the client's commission of a crime or fraud in furtherance of which the client has used the lawyer's services;

confidentiality is a duty of care: lawyers "must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure . . . ."[12]

The duty is not one of strict liability or absolute care.[13] Instead, to determine the appropriate level of care, lawyers are required to balance the risk of harm and likelihood of breach:

> This duty . . . does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule.[14]

Thus, in assessing whether e-mail is appropriate, lawyers must consider the consequences to the client of loss of confidentiality, as well as the likelihood of interception.

This Article addresses the second part of that equation: how likely is it that interception occurs?

> (4) to secure legal advice about the lawyer's compliance with these Rules;
> (5) to establish a claim or defense on behalf of the lawyer in a controversy between the lawyer and the client, to establish a defense to a criminal charge or civil claim against the lawyer based upon conduct in which the client was involved, or to respond to allegations in any proceeding concerning the lawyer's representation of the client; or
> (6) to comply with other law or a court order.

12. MODEL RULES OF PROF'L CONDUCT R. 1.6, cmt. 16 (2003).

13. Were absolute security required, computers could not be used, since they emit radiation that can be "intercepted" from afar. *See* http://www.webopedia.com/DidYouKnow/Computer_Science/2002/vaneck.asp. Nor could lawyers talk on land-based phone lines, since they can be tapped, or talk in their offices, since bugging is possible. *See id.* The possibility of interception is not the issue.

14. MODEL RULES OF PROF'L CONDUCT R. 1.6, cmt. 16 (2003).

IV. THE LIKELIHOOD OF EAVESDROPPING DEPENDS ON HOW E-MAIL IS SENT

This section analyzes the risks associated with the different modes of e-mail communication. E-mail can be sent in various ways, some of which create greater risk than others. This section analyzes the security of various modes of transmitting e-mail, starting with e-mail that does not traverse the Internet, then turning to Internet-based e-mail communications.

A. *Local Area Network Communications*

1. The Risk of Eavesdropping

It is common for lawyers to transmit client confidences by e-mail on "local area networks" or LANs.[15] For example, in-house counsel often use a corporation's internal e-mail system to communicate with their corporate client. Likewise, lawyers in private practice transmit attorney-client information relating to their clients within a law firm over similar closed networks.

Communications which are sent only within a LAN never traverse the Internet.[16] In a sense, e-mail sent over a LAN is little different than a memo delivered by a messenger from one lawyer to another within the same firm. If anything, the e-mail is more secure.

2. Legal Protections

Every person who works in a law firm owes a duty of confidentiality to all firm clients.[17] As a result, because e-mail sent over a LAN may be potentially viewed by all firm employees, every person who may view such information owes an obligation of confidentiality to the firm's clients. Thus the duty of confidentiality is one legal protection afforded to LAN-based e-mail.

In order for a third party to intercept a message on a LAN, the third party would need to gain physical access to the premises and plant a packet sniffer or other interception device on a vulnerable part of the

---

15. *See generally* PRESTON GRALLA, HOW THE INTERNET WORKS, 11 (7th ed. 2004) (describing operation of LANs).

16. *Id.*

17. Every person in a firm owes an obligation of confidentiality to each firm client. *See* MODEL RULES OF PROF'L CONDUCT R. 1.6, 1.0, 5.3 (2003).

network. Absent consent,[18] such conduct is a trespass and is clearly unlawful. Thus, civil and criminal laws protect LAN-based communications as well.

3. Ethics Authorities

Two bar opinions expressly recognized that e-mail transmission wholly within a LAN carries almost no risk of interception. The Illinois Bar Association properly recognizes that "electronic messages that are carried on a local area or private network may only be accessed from within the organization owning the network," and so those "messages would therefore clearly appear subject to a reasonable expectation of privacy."[19] The South Carolina Bar Association likewise recognized the inherently secure nature of LANs:

> Private networks operate on a system accessible only by other computers on the same system (e.g., within the same office) . . . . [M]essages sent from one computer go directly to another computer with no stops in between. This type of communication has been held to maintain a reasonable expectation of privacy. Any inadvertent transmission or intentional interception within a private network would have no effect on confidentiality because all persons with access to that network (i.e. law firm attorneys and employees) owe a duty of confidentiality to all firm clients.[20]

---

18. Firms that permit third parties to have access to internal networks for maintenance must ensure that such third parties contractually agree to abide by the firm's duty of confidentiality. This both avoids any argument of implied consent and establishes a legal duty of confidentiality. Generally, a lawyer may use off-site storage facilities operated by third-parties, provided the lawyer is reasonably assured that the facility will take reasonable precautions to maintain confidentiality. However, no federal law protects these files. *See* N.C. Eth. Op. 209 (1996) ("[A] lawyer should store a client's file in a secure location where client confidentiality can be maintained."); N.Y. Eth. Op. 643 (1993) ("We also see no ethical impropriety in storing closed files . . . so long as client confidences . . . are protected from unauthorized disclosure. The files should be stored in a secure location and should be available only to the client, the client's present or former lawyer, or another with the client's informed consent.") (citation omitted); Mich. Eth. OP. RI-100 (1991) (lawyer may "[s]tore client representation files and other law firm files which are not to be destroyed in a facility which protects client confidences and secrets, safekeeps property, and complies with recordkeeping requirements").

19. Illinois State Bar Assoc. Advisory Op. on Prof. Conduct Op. No. 96-10 (1997).

20. S.C. Ethics Advisory Op. 97-08 (1997) (citations omitted).

Obviously, these conclusions presume that the firm has taken reasonable steps to protect the integrity and security of its LAN,[21] particularly if the LAN is connected to the Internet.[22] These bar opinions do not appear to be controversial, or much disputed. Lawyers can send e-mail on private LANs without violating the duty of confidentiality.

B. *Direct Computer-Computer Transmissions*

1. The Risk of Eavesdropping

It is old hat for lawyers to send and receive confidential information by digital communication over phone lines. Faxes are one example of such computer-to-computer digital communications. Although a misdirected fax may lose its privilege, no one argues that the use of a fax machine or the possibility of misdirection precludes asserting privilege, or has any bearing on confidentiality whatsoever.[23]

E-mail can also be sent directly over land-based phone lines, from one computer to another.[24] When e-mail is sent this way, it is no different than sending a fax. The fact that the lawyer and the client are communicating digitally rather than by voice does not increase the risk.[25] Thus, unless one is willing to say that using a land-based phone line is unreasonable, it is reasonable to use e-mail over direct dial-up connections.

---

21. Obviously, reasonable security measures must still be used. For example, allowing computers which sit in common areas to be unmanned for long periods of time, and without password protection, could allow third parties to review stored communications or e-mail. But that risk is distinct from the risk of transmission itself.

22. *See generally* Ariz. B. Ass'n Eth. Op. 04-05 (2005) (noting that lawyers who store client confidences on computers which are connected to the Internet must take reasonable precautions to protect against inadvertent or deliberate loss of confidentiality).

23. *See* ABA Comm. on Ethics and Prof'l Responsibility Formal Ops. 94-382 (1994) & 92-368 (1992) (indicating that faxes can lose privilege if misdirected). Courts "seem to have taken it for granted" that fax machines may be used to transmit confidential information without violating any ethical rule. ABA/BNA Lawyer's Manual of Professional Conduct § 55:401, at 403 (1996).

24. We doubt anyone does this any more, but in law school in the mid-1980s my best friend and I used modems to connect our computers together over phone lines to communicate. That is what this section is about, and in effect it is no different than facsimile machines. The "modern" analog to this sort of computer-to-computer is the "virtual private network," which is discussed below.

25. Arguably, there is less risk since the person who conducts the wiretap would have to be ready, not just to listen in to an oral conversation, but to intercept a digital communication.

2. Legal Protections

In order to intercept a direct computer-to-computer communication, the eavesdropper would have to place a wiretap on the phone line. This is criminal behavior.[26]

3. Ethical Authorities

The bar associations recognize that e-mail sent over phone lines is secure.[27] No one seems to dispute that conclusion.

C. *Internet Communications*

In order to assess the risks associated with transmitting unencrypted e-mail over the Internet, some background is necessary. When e-mail is sent over the Internet, the risk of eavesdropping is greater than when e-mail is sent over LAN-based or direct computer-to-computer transmissions. This section explains why. Along the way, it also addresses some common misperceptions about e-mail transmission.

E-mail, when sent over the Internet, does not go directly from the sender's computer to the recipient's computer. Instead, once an e-mail leaves the sender's computer, it typically is sent to the sender's router, which has a connection to the Internet.[28] The Internet consists of thousands of separate networks, each connected to each other by routers.[29] Between routers are fiber optic cable and other physical media.[30] These separate networks, connected together by their routers, make up the Internet.

---

26. 18 U.S.C. § 2511 (2002).

27. *See infra* text accompanying notes 113-31.

28. GRALLA, *supra* note 15, at 90-91.

29. Many different router manufacturers exist, including Cisco Systems, Inc., 3Com, Alcatel, Nortel, Siemens AG, and others. In order to simplify this discussion, we generically refer to "routers." Here, "router" is meant to include hardware devices that operate on the "network" layer, layer 3, of the OSI model at point-of-presence gateways. Significantly, "routers" are responsible for forwarding data packets to other routers.

30. *See* STEVE MCQUERRY, CCNA SELF-STUDY: INTRODUCTION TO CISCO NETWORKING TECHNOLOGIES 640-821 (Cisco Press 2004).

The sender's router uses a transmission protocol, typically TCP/IP,[31] to break the e-mail (and any attachments) into "packets" of no more than about 1500 bytes.[32] Each packet is given a "header" identifying its destination, much like an address on an envelope.[33] Each packet is then sent out from the router on to the Internet.

The Internet is a web: often there is more than one route available between two points. More importantly, the path any given e-mail takes between two points may not always be the same. Each packet can take a different path from sender to recipient because most routers on the Internet use dynamic packet routing.[34] Each router's best available path to the destination router may change with every routing table update, based on network congestion, router downtime, or any other number of factors. Depending on which routing protocol[35] any given router uses, these updates will typically take place every thirty to ninety seconds on each router. Considering the incalculable number of routers that make up the Internet, and consequently the possible routes, complete route updates for any given packet probably occur multiple times within a single second.[36]

---

31. Transmission Control Protocol/Internet Protocol, a transport/network layer protocol used to encapsulate data from upper-level protocols, such as SMTP. SMTP, or Simple Mail Transfer Protocol, is an application layer protocol used to transfer e-mail that can only travel over the Internet inside of TCP/IP packets. For more information on the OSI Reference Model, Protocol Data Units, and data encapsulation, see Cisco, Internet Protocols, http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ip.htm; Cisco, IP Routing, TCP/IP Overview, http://www.cisco.com/en/US/tech/tk365/technologies_white_paper09186a008014f8a9.shtml. *See also* SMTP Definition, http://searchexchange.techtarget.com/sDefinition/0,,sid43_ gci214219,00.html (last visited Oct. 4, 2005).

32. *See* Curt Franklin, What is a Packet?, *at* http://computer.howstuffworks.com/question525.htm (last visited Oct. 4, 2005).

33. *Id.*

34. *Id.*

35. Routing protocols are "protocols used by routers to make path determination choices and to share those chioices with other routers." KURT HUDSON & KELLY CAUDLE, CCNA GUIDE TO CISCO ROUTING, at 100-01 (Course Technology, Inc. 2000). Routing Protocols include Routing Information Protocol (RIP), Interior Gateway Routing Protocol (IGRP), integrated IS-IS, Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), and Exterior Gateway Protocol (EGP). *See generally* ALEX ZININ, CISCO IP ROUTING: PACKET FORWARDING AND INTRA-DOMAIN ROUTING PROTOCOLS, ROUTING AND FORWARDING PROCESSES: DYNAMIC ROUTING (2002).

36.

> According to the routing persistence results . . . approximately 10% of the commercial Internet routes had lifetimes of a few hours or less. Moreover, their cumulative distribution function for route lifetimes (based on sampling more than 36,000 host-pairs) was very flat across short time scales. Thus, since routing update protocols are specifically designed to avoid synchronization in the update times, and since the entire Internet contains a huge number of routers, we cannot

Moreover, DARPA (Defense Advanced Research Projects Agency) sponsored research in 2003 concluded that Internet path failures are not "isolated to small set of locations (sic) but seems to be a general property of Internet paths."[37] Path failures are more likely to occur between local neighbor routers, making dynamic routing "particularly important."[38] Internet path failures contribute significantly to packet re-routing; there is an inverse relationship between the frequency of path failures and the constancy of packet routes.

In simpler terms, the sender's router is in contact with the routers which are closest to it. Routers constantly update each other with network conditions and adjust the paths that packets take in light of these changing conditions. In between the routers, the e-mails are in transit in physical communication lines, such as fiber optic cables.[39]

A single e-mail is broken into packets, and each packet may take a different path through the Internet. Once all the packets are received by the destination router, they are reassembled into the original message.[40] Even if the packets are received out of order, they are reassembled into a single coherent original and then transmitted to the recipient's mailbox.[41]

Literature on Internet e-mail security has focused on the Simple Mail Transfer Protocol (SMTP).[42] The focus on SMTP is misplaced. SMTP is

---

> reject the possibility that the mean time between routing updates . . . is below one second.

Thomas Karagiannis et al., *A Nonstationary Poisson View of Internet Traffic*, 8 (2004), *available at* http://www.caida.org/outreach/papers/2004/infocom (last visited Oct. 4, 2005).

37. Nick Feamste et al., *Measuring the Effects of Internet Path Faults on Reactive Routing*, 12 (2003), *available at* http://nms.lcs.mit.edu/papers/failures-sigm2003.pdf (last visited Oct. 4, 2005).

38. Path failures

> are more likely to appear within an autonomous system than on the boundary, thus making reactive routing techniques particularly important. 70% of the failures we observe last less than 5 minutes, and 90% are shorter than 15 minutes . . . Overlay networks can typically route around 50% of failures, independent of failure duration. Overlay networks seem to be more effective at routing around failures between hosts that have at least one large AS along the path.

Id.

39. *See* Nick Pidgeon, *How Ethernet Works*, *at* http://computer.howstuffworks.com/ethernet5.htm.

40. *See id.*

41. *See id.*

42. Harris, *supra* note 5, at 391 ("Long messages may be broken into "packets" which are reassembled at each intermediate system through which the message passes as well as at their final

a protocol within the TCP/IP suite. It is true that e-mail travels through SMTP. However, SMTP is then segmented and packetized by TCP/IP before it ever exits the sender's router.[43] Upon arrival, the recipient router reassembles the TCP/IP packets, allowing the SMTP application layer protocol to take over.

The actual functionality of SMTP mail relays seems to be misunderstood as well. It is true that the SMTP mail relay protocol was designed to store and forward messages indefinitely from server to server until it reached the "delivery" mail server.[44] However, with the advent of open relay exploitation,[45] the only legitimate SMTP mail relays originate from the sender's remote client and only relay once to the sender's domain ("originating") SMTP server.[46] SMTP servers which allow anonymous relay are usually blacklisted in order to prevent the rampant spread of spam mail. Some secured SMTP servers do allow other kinds of mail relay, but the server administrator specifies IP addresses for receiving relays.[47] Arguably, this implies a trust relationship with the relaying client mirroring that of an ISP/customer relationship.

Another common misconception is that the TCP/IP packets are reassembled at each router in between the sender's router and the recipient's router.[48] As noted above, each packet from the sender's router may take a different path to the recipient router. The routers in between do not reassemble the entire e-mail.[49] They simply process the packet they

---

destination."); United States v. Councilman, 418 F.3d 67, 70 (1st Cir. 2005) ("At various points the packets are reassembled to form the original e-mail message, copied, and then repacketized for the next leg of the journey.").

43. *See supra* note 29.

44. RFC 2821, Simple Mail Transfer Protocol (Obsoletes RFC 821), *available at* http://ftp.rfc-editor.org/in-notes/rfc2821.txt (last visited Oct. 4, 2005).

45. *See* John Leyden, *Open Relay Spam is "Dying Out,"* REGISTER, (June 13, 2003), *available at* http://www.it-analysis.com/article.php?articleid=10941 (last visited Oct. 4, 2005).

46. Microsoft TechNet, Restrict Anonymous Access to SMTP, http://www.microsoft.com/technet/prodtechnol/exchange/guides/StopEmailVirus/4486c8c1-8d39-4c83-a8b4-1facc411202e.mspx (2003).

47. *Id.*

48. *See, e.g., supra* text accompanying note 42.

49.

> Routers do not reassemble IP datagrams from IP packets not destined for themselves, for several reasons. First, it would add extra delays in routing: A router would have to wait until all fragments of a given datagram came to it. Second, the router would need to store all fragments of all datagrams before reassembly . . . Third, and maybe most important, because routers perform load sharing — sending packets to the same destination along parallel paths — and because IP packets are sometimes dropped on their way through the network, a router may never receive all fragments of a datagram.

receive, momentarily storing the packet's header and trailer information in the router's volatile RAM, and then forward or discard the packet according to their individual routing tables.

With this background, the vulnerabilities of unencrypted e-mail can be assessed. There are distinct places where e-mail passes through: the sender's and recipient's gateway router, the physical media between the routers, and the routers between the sender and recipient.

An Internet e-mail cannot be intercepted when it is traveling on physical media between routers, such as fiber optic line, any easier than an oral phone call, since it is essentially in the same physical pathway. Accordingly, there is no reason to view the privacy of a digital Internet message when traveling through such physical media any differently than the transmission of a digitized facsimile or an oral telephone call. They are all equally difficult to intercept while in transit. Therefore, the fact that e-mail travels through the physical media that connects the routers does not make it unreasonable to use e-mail unless, again, one is willing to say that using telephones is unreasonable.

With respect to the sender's and recipient's ISPs, the same issues noted below do arise: the lawyer must ensure that his ISP abides by strict policies against monitoring e-mail, and he should consider advising his client to confirm the same with respect to the client's ISP. So long as the ISP is reasonably secure, the use of e-mail should be reasonably safe.

The critical difference between direct computer-to-computer communications and e-mail that traverses the Internet is that Internet e-mail does not go directly from the sender's computer over a land-based line to the password-protected "mailbox" of the recipient.[50] Instead, Internet e-mail goes from the sender through intermediate routers, which are owned by third parties, before reaching the recipient's mailbox.[51]

There are two potential "eavesdroppers." First, monitoring of e-mail by network managers is permitted to a limited extent by the ECPA.[52] Unlike

---

Zinin, *supra* note 35, at 41.

50. *See* Curt Franklin, How Routers Work, http://computer.howstuffworks.com/router.htm/printable.

51. *See* GRALLA, *supra* note 15, at 31.

52. 18 U.S.C. § 2511(2)(a)(I) (2002). This section, which applies equally to phone companies and ISPs, provides:

> It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property

ISP owners, who as discussed below may have contractual obligations to the owner of the e-mail account not to examine e-mail, routers are owned by third parties without any contractual obligation of confidentiality to the sender or recipient of the e-mail.

There can also be unauthorized eavesdropping by third-parties. The principal vulnerability here comes from "sniffing." Sniffing in this context means the surreptitious planting of software on a router to intercept e-mail traveling through a router on its way to the recipient. The routers on which packets travel very briefly hold the packets intended for another router further down the line on the Internet, closer to the recipient.[53] For example, routers on the "backbone" of the Internet look at and move millions of packets of information *every second.*[54] Capturing this information as it is going through these intermediate routers is called "sniffing." Sniffers use software to search for unencrypted e-mail destined to or from certain hosts and copy the message as it goes through the router.[55]

Packet sniffing on a router is infinitely more difficult than sniffing on a LAN. First, remotely installing packet sniffers on a router requires a much more sophisticated attack than LAN sniffing involves. Routers are typically designed to run simple programs specific to routing. Their basic program would not run a typical packet sniffing program.[56] The sniffing program would have to be loaded into a modified firmware program, which sounds just as difficult to accomplish as it actually is.[57] The router would need to be hacked in order to load a modified firmware image. In order to hack a router, one would need to run an RMON (Remote Network Monitoring) probe, DSS (Distributed Sniffer System), a DoS (Denial of Service) attack, or an extremely sophisticated GRE tunnel attack. All of

---

> of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

53. *See* Franklin, *supra* note 51.

54. *See id.*

55. *Cf.* United States v. Councilman, 418 F.3d 67 (2005), *with infra* text accompanying notes 105-11.

56. Router firmware is generally stored in nonvolatile flash memory and router configurations are stored in nonvolatile RAM. *See generally* Cisco IOS Command Line Interface Tutorial, http://www.cisco.com/warp/public/710/lst/IOStutorial.htm (last visited Oct. 4, 2005). Flash memory is also known as EEPROM (electrically programmable and erasable read-only memory). Flash EEPROMs cannot be erased by bytes. They must be erased by the entire chip or large sections of the chip. Jitu J. Makwana & Dr. Dieter K. Schroder, *A Nonvolatile Memory Overview* (2004), http://aplawrence.com/Makwana/nonvolmem.html.

57. Flash memory has a finite number of erase-write cycles, so a router sniffer must be designed to work within this limitation.

these attacks can be prevented using basic system security and proper configuration practices.[58] Of course, no system is invulnerable to attacks, and there have been successful runs of brute force attacks on routers.[59] However, these types of attacks are vastly more sophisticated than installing a simple LAN sniffing program on an end-user client.

Thus, the potential audience for eavesdropping of e-mail on the Internet is made up of (1) those who are lawfully monitoring a router and (2) those who gain unauthorized access, either due to lax physical security of the router or, more likely, by way of using sniffer programs.

With that background on Internet e-mail structure and transmission, the risks associated with transmission of different types of e-mail can be assessed.

D. *Virtual Private Networks or SSL Communications*

1. The Risk of Eavesdropping

Virtual Private Networks (VPNs) and Secure Sockets Layer (SSL) are different but are related means by which private Internet communications can be ensured. As is discussed above, whenever any kind of information — e-mail, web pages, or other files — is sent over the Internet, it is transmitted through intermediate computers. It is possible for third parties to view that information while passing through those intermediate computers.

The combination use of VPN "tunnel"[60] connections with encryption and authentication protocol, such as SSL, prevents those who can capture VPN packets from making any sense of them.[61] A person viewing

---

58. Disabling unnecessary services, ingress and egress filtering, and other fairly simple router configurations can severely disable or cripple most attacks on routers. *See* Improving Security on Cisco Routers, *at* http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml; *Security of the Internet*, 15 FROEHLICH/KENT ENCYCLOPEDIA OF TELECOMMUNICATIONS 231-55 (Marcel Dekker, Inc. 1997); *see also* CERT Coordination Center, http://www.cert.org/.

59. *See* Mark Wolfgang, *Exploiting Cisco Routers*, http://www.securityfocus.com/infocus/1734 (2003).

60. "A tunnel is a logical structure that encapsulates the frame and data of one protocol inside the Payload or Data field of another protocol. Thus, the encapsulated data frame may transit through networks that it would otherwise not be capable of traversing." Cisco, *Virtual Private Networks* (2004), http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/vpn.htm (2004).

61. *See* Stambler v. RSA Sec., Inc., 2003 WL 22749855 (D. Del. Nov. 14, 2003); *see generally* GREG HOLDEN, GUIDE TO NETWORK DEFENSE AND COUNTERMEASURES 295-308 (Thomson Course Technology 2003).

information exchanged through an SSL/VPN connection would see nothing coherent, because the data is scrambled.[62] When used properly, VPNs provide secure means of communication.

However, VPN technology requires that the law firm utilize special enabling software, hardware, or both, and each technology has its own special limitations.[63] For example, for SSL communications, firms must acquire a certificate from an SSL certificate provider.[64] A client who visits an SSL-enabled site can then send information securely.[65] There are other limitations on SSL communications. Foremost, the client must sign on to the firm's site to communicate. The client cannot simply use her normal e-mail program to send a message to the lawyer. This is significant in situations, where for example, one client must communicate with several different law firms.

VPN, like SSL, uses public lines to transmit the communication.[66] Unlike SSL, VPN allows for secure two-way communications. However, VPN requires that both client and lawyer utilize special software.[67]

2. The Legal Protections

The same legal issues concerning e-mail discussed below apply to SSL or VPN communications, since they traverse the Internet. Because they are so difficult to decipher even if they are intercepted, however, any lack of legal protection is of little practical significance.

3. The Ethical Authorities

No opinions addressing whether it was ethical to communicate via SSL or VPN systems were located. However, SSL and VPN are forms of encrypted communication. Therefore, the fact that the bar opinions and commentators consistently agree that, as shown below, encrypted e-mail is secure ought to mean that SSL and VPN communications are, likewise, secure.

---

62. HOLDEN, *supra* note 61.

63. *See* Matthew Syme & Philip Goldie, Optimizing Network Performance with Content Switching: Server, Firewall and Cache Load Balancing, 60 (Pearson Education, Inc. 2004).

64. *See* How Does SSL Work?, http://www.ourshop.com/resources/ssl.html; Window Security, Secure Socket Layer, http://www.windowsecurity.com/articles/Secure_Socket_Layer.html (last visited Oct. 4, 2005).

65. Windows Security, Secure Socket Layer, *at* http://www.windowsecurity.com/articles/secure_socket_layer.html (last visited Oct. 4, 2005).

66. Jeff Tyson, *How Virtual Private Networks Work*, *at* http://computer.howstuffworks.com/vpn.htm (last visited Oct. 4, 2005).

67. *See id.*

E. *Password-Protected Communications Sent Outside the LAN, and with SSL or VPN Systems, Then Within One On-Line Service Provider*

Although it sounds exotic, this section addresses a common means of communication. Lawyers who subscribe to on-line service providers (OSP), such as AOL, typically use a client that creates a proprietary IP tunnel which encapsulates and encrypts packets sent between their computer and AOL,[68] and then send the message to a fellow AOL subscriber. A person may use a computer to communicate over a direct, land-based phone connection to that system. The person can transmit e-mail from his own mailbox (access to which requires a password) to another password-protected mailbox.

1. The Risk of Eavesdropping

There are several differences between LAN communication and communications sent to and subsequently stored on an OSP.

The first difference relates to the way the information is transmitted. If e-mail is transmitted to the OSP over the Internet without SSL or VPN protection, then all of the issues discussed below concerning unencrypted e-mail must be considered.[69] However, ordinarily this is not the case. Many ISPs build SSL or VPN into their communications interfaces, or the connection is dial-up and over land-based phone lines.[70] In the latter case, the message is protected while in transit by encryption or tunneling technology. That is the focus of this section; the use of unsecured transmission is discussed below.

The second difference is where the information is stored. The practical distinction between an OSP and a local area network (such as the law firm LAN described above) is that any member of the public who pays a fee can access an on-line service. An OSP is also subject to "hacking" by nonpaying members of the public.

So long as the e-mail is sent over the Internet by an SSL secured VPN, or dial-up connection, the differences with LAN and OSP e-mail arise

---

68. AOL Webmaster, Connectivity Info (2004), http://webmaster.info.aol.com/connectivity.html; Leslie Ellis, *AOL's Tunneling Conundrum* (2000), http://www.translation-please.com/2000/1113_aol_tunneling.html (last visited Oct. 4, 2005).

69. *See infra* text accompanying notes 99-113.

70. Prior to the advent of broadband, one bar opinion noted that "these services transmit e-mail messages from one subscriber's computer to another computer 'mailbox' over a proprietary telephone network." Ill. St. B. Assn. Advisory Op. on Prof'l Conduct No. 96-10 (1997).

from two facts: (1) the owner of the OSP no doubt can access e-mail stored in its system and (2) because the OSP is connected to the Internet, the site is in a sense a public site and so may be accessed by third parties, such as "hackers" and the like.

2. The Legal Protections

With respect to OSP employee review of stored e-mail, there are two sources of protection. First, an OSP employee who divulges an e-mail, whether stored or in transmission, commits a crime.[71] In addition to criminal laws, lawyers can ensure that the OSP — as with off-site file storage facilities — has a policy in place that protects against review of e-mail.[72] Thus, the legal protection that makes off-site storage facilities ethical to use can come from contract, not just criminal statute.[73]

It is important for a lawyer who is communicating with a client through such a service to consider the system operator's policy toward e-mail: does the system operator consider it to be confidential? AOL's policy toward e-mail was, as of April 2005, as follows:

> We do not use or disclose information about your individual visits to AOL.com or information that you may give us on AOL.com, such as your name, address, email address or telephone number, to any outside companies. AOL.com may share such information in response to legal process, such as a court order or subpoena, or in special cases such as a physical threat to you or others. And, as we

---

71. 18 U.S.C. § 2702(a)(1) (1994) (making it a crime under the Stored Communications Act for persons providing an electronic communication service to knowingly disclose the contents of electronic communications stored by that service).

72. Generally, a lawyer may use off-site storage facilities operated by third-parties, provided the lawyer is reasonably assured that the facility will take reasonable precautions to maintain confidentiality. *See* N.C. Eth. Op. 209 (Jan. 12, 1996) ("[A] lawyer should store a client's file in a secure location where client confidentiality can be maintained."); N.Y. Eth. Op. 643 (1993) ("We also see no ethical impropriety in storing closed files . . . so long as client confidences . . . are protected from unauthorized disclosure. The files should be stored in a secure location and should be available only to the client, the client's present or former lawyer, or another with the client's informed consent.") (citation omitted); Mich. Eth. OP. RI-100 (1991) (lawyer may "[s]tore client representation files and other law firm files which are not to be destroyed in a facility which protects client confidences and secrets, safekeeps property, and complies with recordkeeping requirements"). *See also* ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 95-398 (1995) (discussing access of non-lawyers to a lawyer's internal database).

73. There may be no Fourth Amendment protection for e-mail stored with an ISP without these safeguards. *See* Solove, *supra* note 1, at 20 (explaining that where third-party ISP employees have access to data, it may not be protected by the Fourth Amendment).

> mention above, we may share with our Web site partners aggregated statistical "ratings" information about the use of AOL.com.[74]

AOL's agreement with its subscribers treats e-mail with essentially the same degree of confidentiality required of lawyers. This policy would probably be acceptable if it were part of an agreement made between a lawyer and an off-site storage facility.[75]

In addition, while an on-line ISP could, theoretically, read every single message sent within its system, it is unlawful to do so. Under federal law, a provider of electronic communication services may intercept messages only if it is "in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service . . . ."[76] More critically, if the fact that some monitoring is lawful precludes information from being confidential, then telephone conversations over land-based phone lines are not confidential, because telephone companies are expressly authorized to monitor telephone calls.[77]

With respect to third party access, information stored in password protected e-mail accounts is protected by the Fourth Amendment. As the U.S. Supreme Court stated,

> "[f]or the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not subject of Fourth Amendment protection. . . . But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.[78]

Accordingly, courts have held that e-mail stored on AOL was subject to a reasonable expectation of privacy. One such court stated:

> [A]ppellant clearly had an objective expectation of privacy in those messages stored in computers which he alone could retrieve through the use of his own assigned password. Similarly, he had an

---

74. AOL Privacy Policy (2005), *available at* http://site.aol.com/info/privacy.adp (last visited Oct. 4, 2005).

75. *See* MODEL RULES OF PROF'L CONDUCT R. 1.6 (2003).

76. 18 U.S.C. § 2511(2)(a)(i) (2005).

77. *See id.* (declaring it lawful for a telephone company to monitor telephone calls in the normal course of business).

78. Katz v. United States, 389 U.S. 347, 351 (1967).

> objective expectation of privacy with regard to messages he transmitted electronically to other subscribers of the service who also had individually assigned passwords.[79]

Obviously, the Fourth Amendment applies only to governmental actors, and so this principle simply means that the information is protected from warrantless search and seizure.[80] However, the fact that information protected by a password has been deemed to carry with it an objectively reasonable expectation of privacy suggests that the use of such technology is "reasonable" under Model Rule 1.6.

Even putting the Fourth Amendment aside, unauthorized access by third parties to e-mail stored on an OSP is also a violation of federal law. Specifically, the Stored Communications Act provides a cause of action against any person who "intentionally accesses without authorization a facility through which an electronic communication service is provided... and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage."[81] E-mails that have arrived from the Internet are clearly in "electronic storage."[82] Thus, third parties who intentionally access e-mail that is stored with an OSP before it is read violate federal law.[83]

---

79. United States v. Maxwell, 42 M.J. 568, 576 (A.F. Ct. Crim. App. 1995).

80. *See* United States v. Turner, 169 F.3d 84 (1st Cir. 1999) (holding that a warrantless police search of the defendant's personal computer in his apartment was not justified under the plain view doctrine and therefore violated the Fourth Amendment); United States v. Carey, 172 F.3d 1268 (10th Cir. 1999) (holding that seizure of images of child pornography from defendant's computer hard drive was not authorized by the warrant authorizing search for drug trafficking information); Smith v. Indiana, 713 N.E.2d 338 (Ind. Ct. App. 1999) (holding that a warrantless search and seizure of the electronic contents of the defendant's cellular phone, which had been seized from the defendant's car during an investigatory stop, was not justified under the plain view doctrine).

81. 18 U.S.C. §§ 2701(a)(1), 2707(a) (2005). The Act exempts conduct "authorized . . . by the person or entity providing a wire or electronic communications service." *Id.* § 2701(c)(1). Or, "by a user of that service with respect to a communication of or intended for that user." *Id.* § 2701(c)(2).

82. "[E]lectronic storage" means either "temporary, intermediate storage... incidental to... electronic transmission," or "storage... for purposes of backup protection." 18 U.S.C. § 2510(17) (2005).

83. *See* Freedman v. Am. Online, Inc., 329 F. Supp. 2d 745 (2004) (ISP employee knowingly divulged customer's subscriber information, in violation of Electronic Communication Privacy Act (ECPA), even if employee mistakenly believed that warrant produced by police for information was valid, where employee was aware that ISP was electronic communication service provider, and that customer's subscriber information related to his subscription and thus electronic communications).

3. The Ethical Authorities

Arguably, electronic communications sent over land-based phone lines or SSL encrypted and authenticated VPN connections and then wholly within an external OSP should be considered confidential, provided the OSP provides reasonable network access security. An OSP could meet this requirement by preventing unauthorized access to e-mail accounts by outsiders as well as a policy or agreement with its subscribers that its own employees will not access subscriber e-mail accounts.[84] As one bar association wrote:

> Typically, the computer mailboxes involved are password-protected. Because it is possible for dishonest or careless personnel of the mail service provider to intercept or misdirect a message, this form of electronic mail is arguably less secure than messages sent over a private network. As a practical matter, however, any ordinary telephone call may also be intercepted or misdirected by dishonest or careless employees of the telephone service provider. Again, this possibility has not compromised the reasonable expectation of privacy of ordinary telephone users. The result should be the same for electronic mail service subscribers.[85]

Nonetheless, an opinion from the North Carolina Bar Association ostensibly concluded that e-mail is not secure when sent among OSP subscribers.[86] The opinion addressed the question of "[w]hat is a lawyer's ethical obligation when using electronic mail to communicate confidential client information?"[87] It reasoned:

> E-mail is susceptible to interception by anyone who has access to the computer network to which a lawyer "logs-on" and such communications are rarely protected from interception by anything other than a simple password. In using E-mail, or any other technological means of communication that is not secure, the same

---

84. *See* Susan E. Davis, *Copy, Paste, Send . . . Oops?*, 17 CAL. LAWYER 53 (1997) ("E-mail sent through proprietary e-mail systems (i.e., an intraoffice account such as MCI Mail; a big commercial service, such as AOL or Prodigy; or a direct line between two computers) are safe, because the e-mail stays in a closed loop").

85. Illinois State Bar Assn. Advisory Op. on Prof'l Conduct No. 96-10 (1997).

86. *See* N.C. Proposed Op. RPC 215 (1995).

87. *See id.*

> precautions must be taken as are set forth in [including advising the client of the risks it entails] above.[88]

The South Carolina Bar Association Ethics Advisory Committee also analyzed whether a lawyer could provide legal advice over an "on-line service" without violating the duty of confidentiality.[89] That committee reasoned:

> the very nature of on-line services is such that the system operators of the on-line service may gain access to all communications that occur on the on-line service. Thus, the confidentiality requirements of Rule 1.6 are implicated by any confidential communication which occurs across electronic media, absent an express waiver by the client . . . .
>
> Thus, it is the opinion of the committee that unless certainty can be obtained regarding the confidentiality of communications via electronic media, that representation of a client, or communication with a client, via electronic media, may violate Rule 1.6, absent an express waiver by the client.[90]

Both the North Carolina and South Carolina Bar committees assumed that, by their "very nature," system operators of on-line services have access to all communications that occur on-line. This assumption is false. Certain OSPs agree not to monitor e-mail, as noted above. To the extent that this assumption is false, the conclusion reached does not follow.

Finally, the implications of concluding that OSP use is unethical are profound. For example, the Terms and Conditions of a FedEx USA Airbill — regularly used by lawyers to transmit client confidences — provides: "Right to Inspect: We may at our option open and inspect your packages before or after you give them to us to deliver."[91] If the fact that OSPs have a limited right to lawfully monitor e-mail implicates confidentiality, then surely FedEx's unfettered right to "monitor" means that a lawyer cannot use FedEx, at least not without explaining the risks and alternatives to the client and obtaining the client's informed consent. No practitioners do that. Nor should they be required to do so.

---

88. *See id.*
89. S.C. Bar Advisory Op. 94-27 (1995).
90. *Id.*
91. On file with the author.

For the foregoing reasons, an e-mail sent within an OSP that can be accessed only by the recipient with a password should be held to carry an objective expectation of privacy. As a result, a lawyer who is a member of an OSP that does not regularly read e-mail, can send a message to a client who is also a member of that service over land-based phone lines or VPN/SSL, without violating the duty of confidentiality.

V. E-MAIL SENT OVER THE INTERNET WITHOUT SSL OR VPN CONNECTIONS

There are, broadly speaking, two ways e-mail can be sent over the Internet between OSPs or ISPs: as plain text or in encrypted form.[92] This section analyzes both forms.

A. *Encrypted Internet E-Mail*

1. The Risk of Eavesdropping

Encryption is an electronic "lock-and-key" technology where the lock and the key are made of numbers rather than steel.[93] Encryption programs apply an algorithm to scramble the message.[94] The algorithm itself need not be kept secret; rather, the algorithm allows the user to select an individual "key," which provides the secrecy. The algorithm then uses the key to encrypt the message. In this way, "[c]omputer-based encryption transforms messages into a pattern of letters and numbers using algorithms — mathematical functions that define how to encrypt (encode) and decrypt (decipher) messages."[95] After the user sends the encrypted message, the recipient applies the same algorithm to decrypt the message.

The underlying arithmetic and means of implementing this technology are obviously complex. Nonetheless, software can implement encryption very easily, requiring the user to push a button and enter a limited amount

---

92. Information sent by SSL or VPN connection is encrypted.

93. *See generally* Peter B. Bensinger, Jr., Can the Decrepit Encrypt, Paper Presented at the ABA 22d National Conference on Professional Responsibility, Chi., Ill. (May 30, 1996); David P. Vandagriff, Who's Been Reading Your Email?, 81 A.B.A. J. 98 (1995) (discussing encryption technology); Symposium, Public Key Infrastructure, 38 JURIMETRICS J. 241, 241-514 (1998) (devoting entire symposium edition to public key encryption issues).

94. Stewart A. Baker, *Government Regulation of Encryption Technology: Frequently Asked Questions*, 452 PLI/PAT 287, 290 (1996).

95. Anjali Singhal, *The Piracy of Privacy? A Fourth Amendment Analysis of Key Escrow Cryptography*, 7 STAN. L. & POL'Y REV. 189, 190 (1996).

of text. There are several encryption programs available for commercial use.

Thus, at its simplest, messages are "locked" by the sender, making them unreadable as they pass through the Internet. Until they are decrypted by the intended recipient, who can then decode the message with a key in the form of an electronic password, messages remain unreadable.

2. The Legal Protections

The same legal issues discussed below, concerning whether unencrypted e-mail is protected while passing through a router, also apply to encrypted e-mail.[96] As with SSL/VPN communications, however, because encrypted messages are essentially impossible to read even if they are intercepted, the ease of interception is of little practical import to whether there is confidentiality. Intercepting an unreadable e-mail does not vitiate confidentiality.

3. The Ethical Authorities

All of the authorities recognize encrypted e-mail is secure.[97]

B. *Unencrypted E-Mail*

1. The Risk of Eavesdropping

As the discussion of how Internet e-mail is transmitted demonstrates, e-mail sent over the Internet must pass through the ISP of the sender, the physical media connecting the routers together and ultimately the ISP of the recipient. Each of these risks needs to be assessed.

The ISP of the recipient and sender are obvious vulnerable points. The potential for monitoring by third parties or by the ISP of the sender and recipient means that precautions must be taken, particularly if the messages will be stored in reassembled form. Passwords protect stored e-mail from hackers, and confidentiality obligations of ISPs should preclude monitoring by ISPs of both the accounts of sender and recipient.

Likewise, the potential for "sniffing" for unencrypted e-mail is the same: it is possible to "sniff" for e-mail at routers and surreptitiously learn information in that fashion. Because unencrypted e-mail is sent in plain text, a hacker who intercepts a complete e-mail passing through a router

---

96. *See infra* text accompanying notes 104-12.

97. *See infra* text accompanying notes 112-30.

could potentially reassemble the packets and access the e-mail in an intelligible format.

What kind of "reception" can these potential eavesdroppers get? Reception is, at best, poor. In addition, even when interception is successful, the realities are that often no benefit can accrue to a sniffer because of the obligations of opposing counsel not to misuse an opponent's confidences. Finally, the real-world observable evidence suggests that interception is not occurring.

First, because of the structure of the Internet, sniffing often will result at best in intermittent "reception" by the eavesdropper. The dynamic routing of packets means, first, that not all or even a single e-mail may be processed by a given router (with the exception of the sender's and recipient's gateway routers), and, second, that separate e-mails sent over time between attorney and client are not guaranteed to follow the same path.[98] Furthermore, frequent path failure and on-the-second route updates create severe difficulty in predicting constant packet paths.[99] There is no guarantee, therefore, either that someone attempting to monitor an intermediate router for e-mail between two specific people would see a single packet of a message, or that even if a message between two people was intercepted, that an *entire* message would be seen.

In addition, e-mail travels very quickly. Messages pass through routers in micro-seconds. A packet is typically not present in the router for more than a few microseconds.[100] Absent a pre-planned, sustained effort by a hacker, coupled with the failure of a router administrator to police against sniffing, sniffing is not likely to pick up much information.[101]

The amount of e-mail also serves as a form of protection. The sheer volume of e-mail traffic is incomprehensible. E-mail volume is expected to rise from 2 trillion messages in 2005 to 2.7 trillion by 2007.[102] It would seem likely that any individual who reviewed one isolated e-mail would have a very difficult time putting that information to much mischief, absent unusual circumstances such as a deliberate and sustained effort to obtain the lawyer's e-mail.

Therefore, those monitoring a router would have difficulty eavesdropping on particular messages without actually preparing to do so

---

98. Franklin, *supra* note 51 ("Your e-mail flows over any one of thousands of different routes to get from one computer to another.")

99. *See supra* text accompanying notes 28-59.

100. Franklin, *supra* note 98.

101. *See supra* text accompanying notes 28-59.

102. David Hallerman, *Email: Turning up the Volume*, *at* http://www.imediaconnection.com/content/5630.asp (last visited Oct. 4, 2005).

ahead of time. In light of all of these facts and the shear volume of Internet e-mail, absent a deliberate and sustained attempt to intercept a lawyer's messages, misuse of Internet e-mail will be difficult.

Real world data confirms that sniffing is not something to worry about. As yet, there is no reported case involving sniffing of e-mail by third parties by placing the e-mail on routers. The major insurance companies have advised us that, at present, no claim has been made based upon the interception of an e-mail.

There are perhaps some common sense reasons explaining why sniffing for lawyer-client e-mail does not seem to be occurring. If the goal is making money, there are much easier things to sniff for — credit card numbers being the most obvious. Likewise, a hacker who successfully intercepts an attorney-client e-mail is not likely to be in a position to put the information to much use. For example, were a hacker to intercept an e-mail of a draft brief, most likely the only person to whom that information would be useful would be opposing counsel. Additionally, opposing counsel who receive confidential information of an opponent from an unauthorized source are required in many states to avoid using the information.[103]

Obviously, there are exceptions. Some attorney-client e-mail might be commercially valuable, such as an e-mail disclosing the fact that a company intends to launch a takeover. Nevertheless, the point here is not that some e-mail might be valuable to a hacker. Rather, the point is that on

---

103. *See* ABA Comm. On Ethics and Prof'l Responsibility, Formal Op. 94-382 (1994) (where a lawyer receives confidences from an obviously unauthorized source, he must limit review of the material and advise opposing counsel of receipt); *In re* Shell Oil Refinery, 143 F.R.D. 105 (E.D. La. 1992) (lawyer given confidential documents by employee of opposing party may not use them but must notify opposing counsel), *amended and reconsidered on other grounds,* 144 F.R.D. 73 (E.D. La. 1992). Somewhat similarly, a "lawyer who receives a document relating to the representation of the lawyer's client and knows or reasonably should know that the document was inadvertently sent shall promptly notify the sender." MODEL RULES OF PROF'L CONDUCT R. 4.4(b). A comment to the rule explains that a lawyer who knows or reasonably should know that a document was sent inadvertently should "promptly notify the sender in order to permit that person to take protective measures." The comments also specifically state that the rule covers inadvertently sent e-mail. *Id.* cmt. 2. Ethics opinions in many states also impose duties upon lawyers who receive inadvertently transmitted documents from another lawyer. *See, e.g.*, N.Y. City B. Ass'n Comm. on Prof'l & Jud. Ethics Op. 2003-04 (2004) (concluding that a lawyer who receives misdirected documents must, if it contains "confidences" or "secrets," advise the sender of the mistake, unless the lawyer has a good faith belief that a tribunal before which a dispute is pending will conclude confidentiality has been waived); *see also* N.Y. County L. Ass'n Eth. Comm. Op. 730 (lawyer should assist in preserving confidences of sender of inadvertently privileged documents); ABA Comm. On Ethics and Prof'l Responsiblity, Formal Op. 92-368 (1992) (recipient of misdirected communication should advise sender of the mistake and abide by its instructions).

the whole, attorney-client e-mail does not appear to be a rich source of quick money to hackers. Therefore, sniffing for this type of e-mail is not likely to occur with much, if any, frequency. It is also consistent with the fact that no incident of lawyer-client e-mail interception has been reported, despite the trillions of lawyer-client e-mails that have been transmitted over the Internet without encryption.

For all these reasons, Internet e-mail is subject to interception while in transit. However the realities of the transmission process, the content of e-mail, and the ethical constraints on opposing counsel all point to the conclusion that it is reasonably secure.

2. The Legal Protections

E-mail sent through the Internet passes through three distinct areas: the sender's and recipient's ISPs, the physical media, and the intermediate routers. Each area must be analyzed separately.

As noted above, e-mail stored by an ISP is protected by law.[104] When an e-mail is transiting wires, fiber optic cable, or cable TV wiring, it is illegal to intercept.[105]

The issue of whether e-mail transiting a router is protected by the ECPA is an issue that has caused considerable debate. In late 2004, the First Circuit issued a panel decision, *United States v. Councilman*,[106] in which a two-judge majority reasoned that the ECPA did not apply to e-mail while it was "on" a router, because at that time it was "stored" and therefore not "intercepted."[107]

The circuit court reversed *en banc*.[108] The facts are worth discussing, since the circuit court did not precisely address the intermediate routers. Councilman set up a domain name, "interloc.com," as a bookselling site. He then sold e-mail addresses to other booksellers who wanted to use the domain name. However, unbeknownst to them, he allegedly set up the e-mail system so that copies of certain e-mails bound for his customers were sent to him, so that he could gain a commercial advantage. Eventually, a criminal proceeding was brought against Councilman for violation of the ECPA.

In its *en banc* decision, the First Circuit rejected Councilman's argument that the ECPA did not protect against interception of the e-mails.

---

104. *See supra* text accompanying notes 71-73.

105. *See generally* United States v. Councilman, 373 F.3d 197 (1st Cir. 2004), *vacated on other grounds*, 418 F.3d 67 (1st Cir. 2005).

106. *Id.* at 197.

107. *See id.*

108. *See generally Councilman*, 418 F.3d at 67.

The Court reasoned that at the moment he copied them, they were "stored" in the RAM or hard drives of his e-mail system, while en route to the mailboxes of the recipients. Specifically, the court interpreted the ECPA to apply to e-mail while it is passing through "transient electronic storage that is intrinsic to the communication process for such communications."[109]

Given that the passage of e-mail through routers is "intrinsic to the communications process for" e-mail, the interception of e-mail while passing through a router would violate the ECPA. All of the ethical authorities that support the use of unencrypted e-mail are based, in part, on the premise established in the articles printed eight years ago:[110] that interception of e-mail sent over the Internet violates the ECPA. This is the issue that *Councilman* essentially addressed,[111] and this is the conclusion that it essentially confirmed. Therefore, the importance of *Councilman* to these decisions is worth noting. Again, however, illegality is but one part of the equation: practical difficulty is the other.

3. The Ethical Authorities

a. The Early Opinions

Not surprisingly, the early ethics opinions on the issue of whether lawyers may ethically use unencrypted e-mail reached conflicting results. The first two opinions to address Internet e-mail reasoned that transmission of unencrypted Internet e-mail violated the lawyer's duty to safeguard client confidences and therefore could be done only with client consent.

In the earliest opinion, the Iowa Bar Association (Iowa Bar) reconsidered an earlier opinion[112] and altered its original conclusion regarding the use of the Internet in some measure, but still found that unencrypted e-mail should not be sent over the Internet. The Iowa Bar had been asked to delete the requirement in its earlier opinion "that sensitive material be encrypted in communications between lawyer and client" because, opponents argued, "the Internet provides no greater risk than talking 'over a wire' or using Federal Express."[113] The Iowa Bar disagreed, stating, "[w]hether or not it is no more risky than another medium is not

109. *Id.* at 79.
110. *See supra* note 2.
111. Liebesman, *supra* note 6, at 909.
112. Iowa Bar Association Formal Op. 95-30 (1996).
113. Iowa Bar Association Formal Op. 96-1 (1996).

the question. The question is whether it is risky, and how risky, and at the very best, at this time, this is less than certain."[114] However, the Iowa Bar modified its earlier opinion slightly, stating:

> Pure inter-exchange of information or legal communication with clients is an exception to the Division I of this opinion, but with sensitive material to be transmitted on E-mail counsel must have written acknowledgment by client of risk of violation of DR 4-101 which acknowledgment includes consent for communication thereof on the Internet or non-secure intranet or other forms of proprietary networks, or it must be encrypted or protected by passwords /firewall or other generally accepted equivalent security system.[115]

The factual bases relied upon by the Iowa Bar are, upon close analysis, not at all probative of the issue of e-mail confidentiality. The Iowa Bar relied on a statement that, unless encrypted, e-mail can be read by the router operators.[116] This is indisputable, but it is equally indisputable that switchboard operators and phone companies can listen to phone calls to precisely the same extent, as noted above. If the mere possibility of disclosure to third parties makes written client consent a prerequisite to use of the technology, then lawyers need client consent to use a land-based phone line.

Furthermore, the Iowa Bar Association relied on the fact that neither Visa nor Mastercard currently believed that there was the ability to verify that a person transmitting a credit card number over the Internet was, in fact, an authorized user of that card.[117] This fact has nothing to do with the confidentiality of the transmission, but instead with the verification of the content of the message and identity of the sender.

The assumptions underlying the Iowa Bar opinion are also worth noting. First, the opinion presumes unlawful conduct by the operator in that it presumes the operator will review all information on the router, rather than to the limited extent authorized by the ECPA.[118] Second, although Internet e-mail is subject to review by those who operate the computers, as a part of ordinary monitoring or maintenance, the very same statute permits monitoring of traditional telephone calls. No case has held

---

114. *Id.*
115. *Id.*
116. *See id.*
117. *Id.*
118. *See supra* note 22 and accompanying text.

that this monitoring operates to deny a reasonable expectation of confidentiality.[119] Third, the opinion ignores the difficulty that exists in intercepting a specific Internet e-mail message while it is being transmitted through a router, as discussed above. Moreover, e-mail is transmitted in separate packets, making it even less likely that misuse could occur.[120] Frequent path failures compromise the constancy of any route. This diminishes the probability of an entire e-mail packet flow transiting through any single intermediary router, much less any related communications following the initial packet stream. Any attempt to quantify the probability of route constancy would require selecting the correct abstract Internet topology theory and accompanying algorithm. The Cooperative Association for Internet Data Analysis (CAIDA)[121] is better suited to this task than attorneys and judges are. Route constancy probability is as abstract as chaos theory, and just as fruitful for realistic discussions of interception vulnerability. The better approach to this problem is simple recognition of the fact that frequent path disruptions undermine the reliability of any router interception scheme.

The position of the Iowa Bar would also lead to startling results if applied in legally indistinguishable circumstances. Foremost, a lawyer would have to advise a client that a land-based phone call may not be confidential (due to monitoring), and a lawyer could not send or receive a facsimile from a hotel front desk without risking breach of the duty of confidentiality — even though the Internet operator, unlike the hotel owner, would face criminal liability for disclosing the e-mail.

As a result of these flaws, opinions soon were issued which disagreed with the Iowa Bar.[122] For example, the Arizona Bar Association's opinion stated that "it is not unethical to communicate with a client via e-mail even if the e-mail is not encrypted; this Committee simply suggests that it is preferable to protect attorney/client communications to the extent it is practical."[123] Similarly, in response to "various inquiries regarding ethical issues raised by use of electronic means of communication, including electronic mail and the 'Internet,' by lawyers,"[124] the Illinois Bar explained

---

119. We found no case even rejecting the argument, which says a lot about its weakness.

120. Shea v. Reno, 930 F. Supp. 916, 926 (S.D.N.Y. 1996).

121. *See* CAIDA Web Site, http://www.caida.org/home (last visited Oct. 4, 2005).

122. *See* Pennsylvania Op. 97-130 (1997); Alaska Bar Ass'n Ethics Op. 98-2 (1998); North Dakota St. B. Ass'n Ethics Comm. 97-09 (1997); State Bar of Arizona Advisory Op. No. 97-04 (1997); Illinois State Bar Ass'n Advisory Op. on Prof'l Conduct No. 96-10 (1997) [hereinafter Ill. Bar Ass'n 96-10].

123. State Bar of Arizona Advisory Op. 97-04 (1997).

124. Ill. Bar Ass'n 96-10.

at length why it rejected the conclusions of the South Carolina and Iowa bars:

> Rather than moving directly from the sender's host computer to the recipient's host computer, Internet messages are usually broken into separate "packets" of data that are transmitted individually and re-assembled into a complete message at the recipient's host computer. Along the way, the packets travel through, and may be stored temporarily in, one or more other computers (called "routers") operated by third parties (usually called an "internet service provider" or "ISP") that helps distribute electronic mail over the Internet . . . . To intercept an Internet communication while it is in transit over telephone lines requires an illegal wiretap . . . . The Committee does not believe that the opportunity for illegal interception by personnel of an ISP makes it unreasonable to expect privacy of the message.[125]

In another early opinion, the Vermont Bar Association followed the Illinois opinion and likewise approved the use of unencrypted Internet e-mail, reasoning:

> [A]ll three types of electronic messages (local network, public network, or Internet) appear no less secure than the ordinary fax or telephone communication. For example, e-mail on a local or public network can be accessed only from within the group which owns the network. . . . Undeniably, e-mail sent over public networks and BBS's is potentially less secure than mail sent over a private network because the employees of the public network or an outside person who "cracks" or breaks into the system could intercept the message, but any phone call can be tapped, legally or otherwise, and the mails and faxes can be intercepted and read. Since this possibility of interception also exists for fax transmission and regular mail, no reason exists to treat e-mail differently. . . . To intercept an internet transmission in transit would constitute an illegal wire tap.[126]

In light of these opinions, the South Carolina Bar then re-examined its conclusion that a lawyer could communicate with a client by unencrypted

---

125. *Id.*

126. Vermont Bar Ass'n Advisory Ethics Op. 97-5 (1997).

e-mail only with "an express waiver by the client."[127] The June 1997 opinion concluded that "[t]here exists a reasonable expectation of privacy when sending confidential information through electronic mail (whether direct link, service, or Internet). Use of electronic mail will not affect the confidentiality of client communications under South Carolina Rule of Professional Conduct 1.6."[128] The South Carolina Bar explained the reasons for the change in its conclusion by noting that "[s]ince Opinion 94-27 was issued, the use of e-mail has become commonplace, and there now exists a reasonable level of 'certainty' and expectation that such communications may be regarded as confidential, created by improvements in technology and changes in the law."[129] With respect to unencrytped Internet e-mail, the opinion reasoned:

> Likewise, e-mail transmissions via commercial networks or the Internet maintain confidentiality . . . . The Committee concludes, therefore, that communication via e-mail [maintains] a reasonable expectation of privacy. Because the expectation is no less reasonable than the expectation of privacy associated with regular mail, facsimile transmissions, or land-based telephone calls and because the interception of e-mail is now illegal under the Electronic Communications Privacy Act, 18 U. S. C. §§ 2701(a) and 2702(a), use of e-mail is proper under Rule 1.6.
>
> The Committee notes that a finding of confidentiality and privilege of such should not end the analysis. An attorney owes a client a duty of reasonable care in keeping information confidential . . . . A lawyer should discuss with a client such options as encryption in order to safeguard against even inadvertent disclosure of sensitive or privileged information when using e-mail.[130]

b. The State of the Law Today

The ABA and many states have issued ethics opinions which generally provide that the use of unencrypted e-mail does not, at least in the abstract, violate the duty of confidentiality despite the risk of third-party interception. However, each opinion also warns that under some circumstances plain text e-mail may violate the duty of confidentiality and,

---

127. S.C. Advisory Op. 97-08 (1997).
128. *Id.* (quoting S.C. Advisory Opinion 94-27).
129. *Id.* at 740.
130. *Id.* (citations omitted).

in addition, most require or at least recommend lawyers to consult with the client concerning the use of unencrypted e-mail, or prohibit its use where "sensitive" information is transmitted. Those opinions are:

American Bar Association Formal Op. 99-413 (concluding that there is a reasonable expectation of privacy over unencrypted e-mail but the lawyer should consult with the client and follow its instructions with respect to highly sensitive information).

Alaska B. Ass'n Eth. Comm. Op. No. 98-2 (Jan. 16, 1998) (concluding that a lawyer may use unencrypted e-mail to communicate on "all topics" but admonishing attorneys to "use good judgment and discretion with respect to the sensitivity and confidentiality" of information and advising, but not requiring, that the lawyer caution the client of the risks).

Arizona Eth. Op. 97-04 (Apr. 7, 1997) (stating that "maybe" it is ethical to use unencrypted e-mail, and suggesting that lawyers at least advise clients of the risks).

Connecticut B. Ass'n. Informal Op. 99-52 (concluding that "ordinarily" lawyers may use unencrypted e-mail, but require the lawyer to consult with the client to ensure the client is familiar with the risks it poses and "use good judgment and discretion" in choosing modes of communication).

Delaware St. B. Ass'n Comm. on Prof'l Ethics Op. 2001-2 (2001) (concluding that client consent is unnecessary and that lawyers may use unencrypted e-mail "absent extraordinary circumstances").

District of Columbia B. Ass'n. Op. 281 (Feb. 18, 1998) (concluding that unencrypted e-mail may be used, even absent consent).

Florida Eth. Op. 00-4 (July 15, 2000) (stating that sending unencrypted e-mail "under normal circumstances" is not improper, but stating that an attorney "should consult with the client and follow the client's instructions before transmitting highly sensitive information by e-mail").

Illinois St. B. Ass'n. Advisory Op. on Prof'l Conduct No. 96-10 (May 16, 1997) (stating that encryption is not required, and neither

is client consent, absent "extraordinarily sensitive matters" of a kind that even telephones would be deemed inadequately secure).

Iowa B. Ass'n. Op. 97-1 (1997) (rescinding earlier opinion requiring written permission to use unencrypted e-mail, and instead requiring written acknowledgement to use unencrypted e-mail).

Minnesota Lawyers Prof'l Resp. Bd. Op. No. 19 (Jan. 22, 1999) (concluding that encryption was not required because absolute security is not required).

New York St. B. Eth. Op. 709 (1998) (concluding that "in ordinary circumstances" unencrypted e-mail may be used, but where a particular e-mail is extraordinarily sensitive or is at a heightened risk of interception, encryption must be used). *See also* City of N.Y. Comm. on Prof'l & Jud. Eth. 2000-1 (Jan. 2000) (same); Ass'n. of B. Of City of N.Y. Comm. on Prof'l & Jud. Eth. 1998-2 (Dec. 21 1998) (same).

North Carolina St. B. RPC 215 (July 21, 1995) (concluding that unencrypted e-mail is not unethical, but that a lawyer must use reasonable care and advise the client if using a means of communication susceptible to interception).

North Dakota Ethics Op. 97-09 (1997) (concluding unencrypted e-mail does not violate the duty of confidentiality absent "unusual circumstances").

Ohio Bd. of Comm'r. on Grievance & Discipline Op. 99-2 (1999) (concluding that unencrypted e-mail does not violate the duty of confidentiality, but advising lawyers to "use his or her professional judgment in choosing the appropriate method of each attorney-client communication").

Pennsylvania B. Ass'n Comm. on Legal Eth. & Prof'l Resp. Informal Op. No. 97-130 (Sept. 26, 1997) (concluding that unencrypted e-mail may be used, but only if the client consents to it and the lawyer does not use e-mail to send information that could be damaging to the client without consent).

South Carolina B. Op. No. 97-1 (1997) (reversing earlier position, which required "certainty" that communication would not be

intercepted, and instead concluding that there is a reasonable expectation of privacy over unencrypted e-mail, and so using it does not violate the duty of confidentiality).

Tennessee Advisory Eth. Op. 98-A-650 (Nov. 1998) (unencrypted e-mail is permitted only if the client has consented).

Utah St. B. Eth. Advisory Op. 00-01 (March 9, 2000) (concluding that a lawyer may "in ordinary circumstances" use unencrypted e-mail, but stating that if the information is "particularly sensitive," or if the lawyer "has reason to believe the risk of interception of the communication is higher," the lawyer should use a more secure means of communication, and that the lawyer "may wish to advise the client at the time he is retained that the lawyer intends to use unencrypted e-mail").

Thus, as of today, no bar association prohibits unencrypted e-mail, and those that once did retracted their earlier positions.

VI. CONCLUSION: LAWYERS STILL WORRY TOO MUCH

The conclusion that lawyers can confidently use unencrypted e-mail rests upon two notions: that it is illegal to intercept, and that when the e-mail is transiting the Internet, it is difficult to intercept. *Councilman* addresses the first notion, and recognizes that intercepting e-mail while "in transit," even if momentarily "stored," violates the ECPA. That should provide some comfort for lawyers.

However, the legal component is only one part of the equation. Even if interception is illegal, if it is easy to intercept messages, the law is of cold comfort to clients and counsel. In this regard, focus on Judge Learned Hand's seminal opinion in *Hooper*[131] is appropriate. Judge Hand recognized that merely because an industry had not generally adopted the precaution of having radio receivers on board tugs so that the tugs could receive weather reports the failure to do so could still constitute a breach of duty.[132]

Is encryption the radio on the tug boat? Not today. Will it be one someday? Perhaps — if there are established risks and little legal protection.

---

131. 60 F.2d 737 (2d Cir. 1932).

132. *Id.* at 740.

There are real risks of communicating over the Internet — just as there are real risks in using the phone, FedEx, computers, mail, or in engaging in "private" office conversations. As of right now, it is reasonable to believe that the nature of the Internet — the packetization, the random routing, and the difficulty of effectively sniffing for messages — makes the continued use by lawyers of unencrypted e-mail acceptable for all but the most sensitive information. No empirical evidence suggests otherwise. Therefore, lawyers should stop worrying and use Internet e-mail.