EMERGING ISSUES ON THE INTERNET FOR THE LEGAL PROFESSION

by Rosaria Vigorito

Introduction

With the growth of the Internet and the exciting advantages of law firms using it in their practice, the legal profession is being radically transformed in the way in which it operates. Many big international law firms electronically transmit documents via the Internet among their various offices and clients throughout the world. Even the smallest law firms, in turn, contemplate the ways to use the Internet to solicit business, communicate with clients and conduct legal transactions via the Internet.[1] Across the board, law firms are setting up Web sites and Extranets; publishing electronic newsletters; using email to correspond with clients and colleagues, and participating in Internet chat rooms and listservs.

Notwithstanding the wonderful advantages of using the Internet and the technology that comes with it, law firms are confronted with many issues particular to the practice of law in adapting to the electronic age. For example, whether the level of security of their email systems adequately protect confidentiality and the attorney-client privilege,[2] whether their Internet connections are secure, whether their Web site activities constitute unauthorized practice of law, and whether information retrieved from the Internet is reliable.

---

[1] See Small Law Firm Technology Survey: 1998 Survey Report, ABA Legal Technology Resource Center (1998); and, Large Law Firm Technology Survey: 1998 Survey Report, ABA Legal Technology Resource Center (1998).

[2] Internet Guide for New York Lawyers 146-147 (New York Bar Association 1999).

However, with the introduction of each new technology preceding the Internet, the legal profession has also undergone transformation and been confronted with new challenges. Legal and ethical issues were raised, for example, with the advent of the telegram, the fax machine and the cellular telephone.[3] In fact, generally email communications are more secure than fax transmissions. Arguably a fax can more easily be sent to an unintended party given the room for error in dialing a phone number. Instead, an email address stored in one's email address book makes it less likely for an email to a saved email address to be misdirected. Yet email communications are subject to their own set of security vulnerabilities.

The following will be an overview of the emerging issues raised by the Internet in the legal profession. In particular, the extension of the attorney-client privilege; the application of the ethics principle of confidentiality to email communications; Internet connectivity and the security issues pertaining to it; and, general "cyberlegalethics" concerns raised by using the Internet, such as avoiding the unauthorized practice of law and verifying information found on the Web.

Email

Many law firms have expanded their use of electronic communications to include electronic mail, commonly known as email. Emails are digital messages, which travel through different paths on the Internet in dispersed data segments

[3] John Christopher Anderson. Transmitting Legal Documents Over the Internet: How to Protect Your Client and Yourself, 1 Rutgers Computer & Tech. L.J. 1, 3-4 (2001).

or packets and "travel through a series of routers, computers and networks,"[4] until they reach their destination, where they get rejoined into coherent messages.[5] In contradistinction, faxes are transmitted in analog form and are not encoded or scrambled, so the document travels as a whole.

There are different ways to connect via email. These include Intranets, which work within an organization and allow only for internal access. There are also direct modem-to-modem connections between private parties. Some Extranets[6] work this way, whereby a private network directly dials into another private network. The general way to connect, however, is either via online service providers, whereby the email system provider issues passwords to its users, or via a general Internet service providers ("ISP") that include local and various sized providers.[7]

Unlike its predecessors, there are several advantages of email transmissions. They are a very convenient mode of communication. Regardless of the time of day or the location,[8] a document can be sent to a known recipient or a number of recipients. It is also faster than other modes of communication. Multiple recipients can be reached with one transmission and at incredible

---

[4] Id. at 5.

[5] See Karen M. Coon, Comment, United States v. Keystone Sanitation Company: E-mail and the Attorney Client Privilege, 7 Rich. J. L. & Tech. 30, ¶ 8 (2001) (visited March 7, 2001) http://www.richmond.edu/jolt/v7i3/article4.html.

[6] Extranets, which are discussed infra, are growing in popularity and will be used for such purposes such as providing clients with billing records and opposing counsels with required documents retrieval. See, Dennis Kennedy, Law Firms Play Catch-Up: Key Legal Technology Trends for 2002 (visited Jan. 10, 2002) http://www.llrx.com/features/techtrends2002.html.

[7] See Coon, supra note 5, ¶¶ 8-13.

[8] Provided one is connected to the Internet provider and can access one's email account.

speeds. Email communication is also cost-effective and inexpensive.[9]

1. Attorney-Client Privilege

Notwithstanding the seeming secure mode of transmission, email communication security is vulnerable. Inadvertent reading of firms' emails to clients by third parties occurs by way of misdirection, unlawful interception or mishandling of email storage. These issues are troublesome and must be addressed by firms. Moreover, emails are generally discoverable under state and federal rules of evidence,[10] unless they are protected correspondences under the attorney-client privilege.[11] Hence, firms must have policies that are geared to ensure that the said correspondences do not lose their attorney-client privilege status.

On the statutory level, federal regulation of Internet communications is covered under the Electronic Communications Privacy Act of 1986 ("ECPA").[12] The ECPA prohibits the unauthorized intentional interception, use and/or disclosure of any wire, oral or electronic communication. Intentional access or disclosure of email, without authorization or court order is subject to civil and criminal liability.[13]

In New York State ("NYS"), Civil Practice Law and Rules ("CPLR") § 4548 specifically extends privilege status to communications made by email. It

---

[9] See Coon, supra note 3, ¶¶ 23-24.
[10] Internet Guide, supra note 2, 147-48, which cites to Article 31 of the CPLR and Rule 26 of the Federal Rules of Civil Procedure.
[11] Treatment of an email message is not contingent on its format, i.e., electronic or printed, but rather on its content.
[12] Pub. L. No. 99-508, 100 Stat. 1848 (1986), codified as amended at 18 U.S.C. §§ 2510 et seq.

provides that “[n]o communication privileged under this article shall lose its privileged character for the sole reason that it is communicated by electronic means or because persons necessary for the delivery or facilitation of such electronic communication may have access to the content of the communication.”[14] Affording privilege status to email communications helps ascertain if they are discoverable or admissible in court.

The attorney-client privilege is created whenever there are communications, conversations, advice and information shared between a "client" and an attorney, in her or his professional capacity. Such exchanges, unless expressed waived by the client, are protected under the Federal Rules of Civil Procedure (“FRCP”) and under the CPLR. However, under the FRCP or the CPLR, matters that are deemed not privileged are discoverable. Hence, upon a discovery request for such servers and back up disks, emails messages which were thought to have been permanently erased by the firm, may be retrieved and used if they do not fall under the attorney-client privilege.

To properly protect themselves, firms must develop document retention and destruction policies that are in place. This includes wipe programs,[15] which permanently remove email messages from the server hard drives, rather than just deleting them. When a user deletes his or her messages, they are not deleted from the network server because they still rest on the server until they

---

[13] 18 U.S.C. §§ 2701-2711.
[14] Penal § 250, instead, imposes criminal liability to intentional interceptions and disclosures of electronic communications.
[15] See Internet Guide, which makes reference to “wipe programs” and the Department of Defense approved standards programs. Id.

are written over. Further, many firms also have back up systems, whereby supposed it deleted messages still rest intact on those back up disks.

Care must be taken to develop destruction and retention policies for email messages. Included in those policies, however, are efforts not to engage in the activity of spoliation, whereby evidentiary emails are deleted during litigation or while litigation is pending.[16] Courts treat spoliation in a variety of ways and consider a variety of factors. Those factors include whether there was willfulness and intent behind the destruction, whether the duty to preserve during litigation was reasonably foreseeable, and whether the spoliator's activities cause prejudice to the other party.[17]

2. Principle of Confidentiality

However, in addition to the statutory protection of email communications, including the extensions of privilege status to those that qualify, the legal profession is also held to its own professional standards. It is not only bound and protected by statutory parameters, but is also held to the rules of ethics and professional responsibilities of the American Bar Association ("ABA") and the New York State Bar Association ("NYSBA"). Specifically, each of those professional bodies provides rules and duties concerning the principle of confidentiality and privacy and, those rules and duties extend explicitly and implicitly to email communications.[18]

---

[16] Richard J. Wegener, Ethical Issues in the Distribution Context: Destruction of Evidence, Product Distribution and Marketing 1193 (ALI-ABA March 9, 2000).
[17] Id.
[18] The following are sites dedicated to the collection and sharing of ethics-related materials be it related to the Internet or not:[18]

Generally, under Rule 1.6 of the ABA Model Rules of Professional Conduct ("MRPC"), lawyers are ethically bound to preserve the confidences of their clients, i.e., "[a] lawyer shall not reveal information relating to representation of a client unless the client consents after consultation, except for disclosures that are impliedly authorized in order to carry out the representation." The confidential nature of such client information is to be preserved even once the attorney-client relationship ends.

Specifically, however, with the rise of email correspondence between firms and their clients, issues of confidentiality and the unique security risks the Internet poses needed to be addressed. The ABA, in Formal Opinion 99-413, entitled "Protecting the Confidentiality of Unencrypted Email," did just that and found:

> [e]mail communications, including those sent in encrypted over the Internet, pose no greater risk of interception or disclosure than other modes of communication commonly relied upon as having a reasonable expectation of privacy. The level of legal protection accorded email transmissions, like that accorded other modes of electronic communication, also supports the reasonableness of an expectation of privacy for unencrypted email transmissions. The risk of unauthorized interception and disclosure exists in every medium of communication, including email. It is not, however, reasonable to require that a mode of communicating information must be avoided simply because interception

---

> •The American Legal Ethics Library (visited March 4, 2002) http://wwwsecure.law.cornell.edu/ethics, from Cornell's Legal Information Institute. Available at this site are fulltext of or links to most states' professional codes and the ABA's model code.
> •The ABA Center for Professional Responsibility (visited March 4, 2002) http://www.abanet.org/cpr/home.html. This site provides fulltext materials such as the Model Rules of Professional Conduct, opinions of the ABA's Standing Committee on Ethics and Professional Responsibility, and information on multidisciplinary practice and multi-jurisdictional practice.

See Robert Ambrogi, Let's Get Ethical on the Web, New York Law Journal, Monday, February 4, 2002, vol. 227, no. 23, t7, col. 1.

> is technologically possible, especially when unauthorized interception or dissemination of the information is a violation of law.
>
> The Committee concludes, based upon current technology and law as we are informed of it, that a lawyer sending confidential client information by unencrypted email does not violate Model Rule 1.6(a) in choosing that mode to communicate. This is principally because there is a reasonable expectation of privacy in its use.

Hence, the ABA reasoning was that since the ECPA prohibits the illegal interception of email communications, then email communications remain private, even if improperly intercepted and without encryption.

Even so, the ABA also stated:

> When the lawyer reasonable believes that confidential client information being transmitted is so highly sensitive that extraordinary measures to protect the transmission are warranted, the lawyer should consult the client as to whether another mode of transmission, such as special messenger delivery, is warranted. The lawyer then must follow the client's instructions as to the mode of transmission.

In New York, under the NYSBA Disciplinary Rule 4-101(B), a "lawyer shall not knowingly … reveal a confidence or secret of a client." By extension, DR 4-101(D) provides, a "lawyer shall exercise reasonable care to prevent his or her employees, associates and others whose services are utilized by the lawyer from disclosing or using confidences or secrets of a client."

The Committee on Professional Ethics of the NYSBA, in turn, with Opinion 709, dated September 16, 1998, discussed, among other things, the use of email by a firm. It believed that the existing federal and state statutes criminalizing unauthorized interception of email enhanced the reasonableness of email communications being "as private as other forms of telecommunication." In fact, the Committee went on to say, "[w]e therefore conclude that lawyers may in

ordinary circumstances utilize unencrypted Internet email to transmit confidential information without breaching their duties of confidentiality under Canon 4 to their clients, as the technology is in use today."

Nonetheless, the Committee also went on to say:

> [d]espite this general conclusion, lawyers must always act reasonably in choosing to use email for confidential communications, as with any other means of communication. Thus, in circumstances in which a lawyer is on notice for a specific reason that a particular email transmission is at heightened risk of interception, or where the confidential information at issue is of such an extraordinarily sensitive nature that it is reasonable to use only a means of communication that is completely under the lawyer's control, the lawyer must select a more secure means of communication than unencrypted Internet email.

Hence, although the foregoing ABA and NYSBA standards on email communications encourage the use of email and believe such use is afforded a the reasonable expectation of privacy because of the criminalization of unauthorized interception, firms are still under the duty to protect the confidentiality of their clients' information. In fact, the duty to preserve clients' confidences and secrets is considered greater than the evidentiary attorney-client privilege.[19] NYSBA's Ethical Consideration, i.e., EC 4-4 provides, "[t]he attorney-client privilege is more limited than the ethical obligation of a lawyer to guard the confidences and secrets of the client. This ethical precept, unlike the evidentiary privilege, exists without regard to the nature or source of information or the fact that others share the knowledge." However, this is not a strict liability duty.[20]

The seeming secure mode of transmission, email communication security

[19] Internet Guide, supra note 10, 146.

is vulnerable not just to devices used by hackers[21] but also in other less thought of ways. For example, as emails travel through cyberspace, technically their access by the Internet service providers is possible. Moreover, emails are oftentimes stored in the recipient's server or desktop inbox or folder until they are opened and deleted. These factors, in addition to the deletion issue mentioned supra, potentially leaves room for confidentiality breaches.

Hence, the responsibility is on a firm to protect itself from any prospective breach of confidentiality. Practical ways to reasonable protect itself includes a firm policy to first and foremost obtain its clients' permission to use email communications. In fact, many state bar associations recommend obtaining client consent for engaging in email communications in addition to obtaining consent from clients before disclosing any confidential information.

Permission to use email and other electronic communications may also be accomplished with initial retainer documents. Language might include the following, "Our office uses one or more of the following technologies in its day-to-day operation: cell phone, email, facsimile and Internet. Your signing this letter of engagement shall constitute a consent to use these communication devices in your matter."[22]

Notwithstanding the getting of initial client permission to use email communications, however, when dealing with sensitive documents, during the course of handling a client's affairs, it is recommended that there be consultation

---

[20] Internet Guide, supra note 10, 146.
[21] Discussed infra.
[22] Internet Guide, supra note 10, 147.

as to their mode of transmission. In fact, consultation with the client can be revisited each time, as deemed necessary. However, a good rule of thumb would be more sensitive the documents are, the greater need for more secure modes of transmission.

Additional measures include the use of legal disclaimers or confidentiality notices on email transmissions. A notice would not absolve the firm of its duty to its clients nor be construed as an admission that such transmissions were unsecured, but rather, might protect the firm. Suggested language would include the following:

> The information contained in the email is intended for the use of the named recipient only. It may contain information that is privileged, confidential and exempt from disclosure under applicable law. If the read of this message is not the intended recipient, or the employee or agent responsible for delivering this message to the intended recipient, you are hereby notified that any use, dissemination, distribution or copying of this communication is strictly prohibited. If you have received this communication in error, please notify us immediately by email, by using your reply button to advise us of such error. Thank you.[23]

3. Encryption and Other Security Measures

Notwithstanding the foregoing, including obtaining client consent to email correspondence and using disclaimers on email transmission, a firm may also procure encryption software to protect against the growing prevalence of "email wiretapping" and the like.[24] Hackers are devising more and more creative ways to intercept emails, including composers of emails can get copies of the

---

[23] Id.

[24] Jeffrey Beard, Email Snoopers' Powerful Tools Threaten Electronic Privacy, The National Law Journal, published March 26, 2001 (visited Jan. 10, 2002)

recipient's replies and forwarded messages to bounce back to them.[25] Even with the attorney-client privilege protection and the other laws against unlawful interception of email, a hacker may use the information obtained to hurt a firm and/or its clients outside of the legal proceeding.[26]

Of the hackers' key tools are packet sniffers.[27] These software programs can screen through large quality of emails, looking for certain words, names or numbers. There is a growing sophistication of email sniffer programs and facility in which they can analyze large volumes of email. The Federal Bureau of Investigation, for example, uses a program known as Carnivore, which is able to sniff out emails, file download and chat-room conversations, by scanning millions of email messages per second.[28] In turn, hackers are developing and employing snooping programs. As a result, the email snooping danger becomes a real concern particularly for large law firms and firms that handle cases involving a

---

http://www.law.com/cgibin/gx.cgi/AppLogic+FTContentServer?pagename=law/View&c=Article&cid=ZZZQPILWMKC&live=true&cst=1&pc=0&pa=0.

[25] Id. Notwithstanding, this bounce back interceptive activity is based on certain pre-requisite factors, such the email being written in HTML and the email program is operating with JavaScript enabled. This includes Microsoft Outlook and outlook Express, Netscape 6 Mail, America Online 6.0 and the latest Eudora programs. All the hacker needs to do is code the JavaScript and vuola. Those programs that have JavaScript disabled or do not have it at all are not vulnerable to this type of hacking activity.

What compounds this problem, though, is that the security of an email system is contingent on the JavaScript setting of any of the people in the chain of emails. Presumably, sending an email in plain text would circumvent this problem.

[26] Jerry Lawson, Six Email Security Myths, Internet Tools for Lawyers (visited Jan. 10, 2002) http://www.newlawtools.com/security/six_myths.htm.

[27] Jerry Lawson, The Complete Internet Handbook for Lawyers, ABA Law Practice Management Section (1999), 223.

[28] Anderson, supra note 3, 10-11.

significant amount of money.[29] According to one authority, "[t]he low risk of being detected, let alone caught, let alone prosecuted and punished, makes email snooping much more attractive to sophisticated snoops than the alternatives. Further, email snooping can be enormously cheaper than other methods of snooping."[30]

Another email concern is the use of forged email, also known as spoofing. According to one author, "[e]mail with falsified return addresses may be used to trick an email recipient into releasing confidential information … If the unknowing attorney were to do so, he or she could destroy the privileged nature of such communications and could incur ethical problems."[31] An example of spoofing occurred in 1998 to LexisNexis, when an email scam involving imposters purporting to act for the company requested customers to email their LexisNexis passwords to a generic email address.[32]

The problem of forged emails is possible because the recipient of an email is not able to identify or is confused as to the identity of the sender. Hence, unless there is a method with which to properly ascertain the sender's identity, the recipient may be communicating and forwarding sensitive materials and documents to an unauthorized third party.

Firms can invest in efforts to secure email communications with the use of encryption programs. Encryption is a defense against snooping or targeted

---

[29] Jerry Lawson, An Email Security Primer for Lawyers, Part I: Do you Ever Need to Encrypt Your Email? (visited Jan. 10, 2002) http://www.netlawtools.com/security/emailsecurity1.html.

[30] Id.

[31] Anderson, supra note 3,14.

attacks.[33] It is an electronic security system that uses a mathematical encoding and decoding formula, to protect the transmission of an electronic communication, whereby, without the ability to decrypt a message that has been encrypted, the text of the email is in unreadable gibberish. The recipient of such an encrypted email uses a key that interprets the code and reveals the message sent.[34]

Traditionally, the problem with encryption software has been they require both parties, i.e., sender and recipient, to have the same software and the keys need to be programmed. Further, the software is expensive and uses a lot of computer memory.[35] It also is not tamper proof.

The rise of public key encryption has overcome some of these problems. First, they are more secure and provide greater convenience. The latter is accomplished with a dual key system, whereby one key is public and the other private. For example, the firm would hold the private key, whereas the public key would be made available to clients.[36] A commonly used system that is accepted in ebusiness sites is the 128-bit encryption provided by a "Secure Sockets Layer" ("SSL").[37] Some firms are using PGP ("Pretty Good Privacy") or similar public key encryption programs to secure their email messages. An example of a

---

[32] Id. at 3-4.
[33] John Heckman, Internet Security: What You Need to Know to Protect Your Firm, Microlaw (visited Jan. 10, 2002) http://www.microlaw.com/columns/guest/heckman1.html.
[34] Coon, supra note 5, ¶¶ 51-58.
[35] Id.
[36] A public key consists of a long block of random numbers and letters, which the software attaches to the sender's message. See Lawson, Complete Internet Handbook, supra note 26, 225-237. Other types of encryption programs are also discussed.

public key is as follows:

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.7

mQBtAy90aHoAAAEDAM08EwnPG8yCYBKnCT8viqLdZP4XdI2fFXUx/td
S/3nR2UFKfpLKjhANgEovdQfPlkLbuUZnrrZuKRR8o3G7rIfuyYvkqbsMnV
QjEJ3eWGmT/FsYFqMRSFOvDWCpbRpcSwAFEbQqU3VuYnVyc3QgQ2
9uc3VsdGluZyA8c3VuYnVyc3Rabm92yW51dc5jb20+
=o//1

-----END PGP PUBLIC KEY BLOCK-----[38]

Related security measures include the use of digital signature. This is used for authentication and security. Digital signatures are used to verify the sender of an electronically transmitted document and may also be used to verify the authenticity of the contents of that document. Public key encryption facilitates the use of digital signatures.[39] The sender uses a private key to encrypt the message and the recipient uses the sender's public key to decrypt it. Only if the sender's public key decrypts the message is it verified that the message came from that person. An example of a digitally signed document is as follows:

-----BEGIN PRIVACY-ENHANCED MESSAGE-----
Proc-Type: 2001, MIC-CLEAR
Originator-Name: webmaster@www.sec.gov
Originator-Key-Asymmetric:
MFgwCgYEVQgBAQICAf8DSgAwRwJAW2Snkk9AvtBzYZmr6aGjl
WyK3XmZv3dTINenTWSM7vrzLADbmYQaionwg5sDW3P6oaM5D
3tdezXMm7z1T+B+twIDAQAB
MIC-info: RSA-MD5, RSA,
WQOsKpTDrq1aLZm4FPSlsf0ubj8u52KFSaTJb+m3296XtUmXyuy
RYehh8DP-odWpvG6SpGP916CZWMW1nw11A==

---

[37] Heckman, supra note 32.
[38] Lawson, Complete Internet Handbook, supra note 26, 228.
[39] Id. at 235.

> [The body of the digitally signed message goes here]
> -----END PRIVACY-ENHANCED MESSAGE-----[40]

Digital signatures can be used to authenticate the identity of an email sender. A digital signature is not a computerized version of one's signature, but rather, it is "a term of art describing a systematic scrambling of characters to guarantee security and authenticity."[41] The use of a digital signature on a transmitted document enables the recipient of the document to verify the identity or the email sender and the authentication of the document's contents. In fact, the use of digital signatures,

> authenticates the entire document down to the last punctuation mark …Therefore, the documents' contents are practically impossible to alter without detection … Further, electronic documents can be encoded with digital time stamps, which allow the transmission time to be ascertained … Finally, digital signatures eliminate the possibility that the sender will successfully repudiate or deny having sent the document.[42]

In accommodating to this new technology, the ABA released guidelines in August 1996, entitled, ABA Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce.[43] Subsequently, NYS passed legislation to facilitate the use of digital signatures in ecommerce.[44] Specifically, on September 28, 1999, it enacted the State Technology Law,

---

[40] Id. at 235-236.
[41] Anderson. supra note 3, 35.
[42] Id. at 36-37.
[43] Prepared by the ABA Section of Science and Technology Information Security Committee.
[44] In June 1999, the Electronic Signatures in Global and National Commerce Act was signed by President Clinton, which tried to reconcile this area nationwide. States may preempt this federal law if they opt to adopt the July 1999 National Conference of Commissioners on Uniform State Laws' Uniform Electronic Transactions Act, or if they opt to pass a law that is technologically neutral.

which includes Article I: New York Electronic Signatures and Records Act,[45] wherein an electronic signature may be used in place of a hand affixed signature, and have the same legal validity and effect of a hand written signature. The following year, effective October 18, 2000, the Office of Technology promulgated the New York Electronic Signatures and Records Act Regulations, 9 NYCRR Part 540, which was implemented to establish standards and procedures governing the use and authentication of digital signatures.

Overall, the statute and regulations enable New York citizens, businesses, state and local governments to use electronic signatures or electronic records. Notwithstanding, the electronic signature must, however, comply with certain standards in order to meet the regulatory requirements. It cannot be a signature that is easily duplicated, is unique to the electronic signatory, is capable of verification, is under the sole control of the person using it, and has the same force and effect as handwritten signatures. Hence, digital signatures provide firms with a means with which to identify the parties to an email, a transaction and a document.[46]

Finally, a firm can use, as one writer put it, "common sense."[47] As discussed, if the document involved is of a highly sensitive nature, a firm might consult with its client and consider using a more secure mode of delivery, such as hand delivery, rather than electronic or fax, for that matter. Overall, a law firm needs to ask what, realistically, are its security concerns. What is the likelihood

---

[45] N.Y. State Tech. §§ 101-109.

[46] Further, authentication may in the future be done by way of other technologies, such as biometrics . See Heckman, supra note 32.

that there will be unauthorized access to its electronic transmissions? Further, what will be the consequences if such unauthorized access occurs? The answers to these questions may also assist, if the firm has already decided to purchase encryption products, to determine what type of product best serves that need. Other considerations are to select a product that is easy to use, widely used, that has an adequate level of protection, and that has a key recovery function.[48]

Given that the ABA and the NYSBA have not created an ethical obligation to encrypt, law firms are not required to encrypt to avoid liability.[49] The standard that has been created is that of "reasonable means". If a firm uses reasonable means to protect its clients confidences, including obtaining the clients' informed written consent to use such communications; has a clear email retention policy; perhaps offers encryption as an option to its clients; and, uses confidentiality notices, an example of which is provided supra, similar to those used for faxes, in the transmission of emails; then employing these reasonable means, the firm is meeting the minimum legal and ethical standards.

4. **Related Email Security Issues**

Virus threats posed by hackers are another threat to security. The best way to handle these threats is through education and awareness; and, through

---

[47] Coon, supra note 5, ¶¶ 51-58.

[48] Daniel E. Orr, Confidentiality in an Electronic World Using Encryption in Everyday Law Practice, Network2D, ABA Law Practice Management Section (visited Feb. 1, 2002) http://www.abanet.org/1pm2/newsletters/net2d/s98orr.html. The key recovery function refers to the ability to get a copy of the encrypted password should there be a need to in the event of loss or suspected wrongdoing.

[49] Id.

the proper configuration of software to close security holes and the keeping of updated anti-virus software. [50] The currency of anti-virus software is particularly crucial as hackers are developing new viruses everyday, including those that can spread without even opening an email message.[51]

Besides email security and privacy issues, the managing of email communications is also of concern. According to one expert, email "has already created storage and bandwidth problems for many firms. But the biggest issue for many firms is simply finding ways to ensure that emails are made part of the client 'file.'"[52] In other words, if the emails are printed out, then the issue is simple in that the documents are handled as the other documents and hence filed the same way. However, when the emails are sitting in electronic format on someone's computer and/or the firm's server, how long do they stay there? Are they electronically filed? How are they filed? Should they be kept at length in electronic format at all? Should someone be in charge of overseeing that emails that may have been sent to different attorneys and professional staff at the firm be retrieved and stored in one "file" electronically? Should all documents be stored electronically via document imaging tools?

Then there are concerns over firms losing emails, documents and other sensitive materials on their hard drives and servers to viruses, and in being inundated by spam email messages. There may be an increased need for software and services to counter such concerns. Practice management software

---

[50] Id.
[51] Id.

will assist firms in managing many of these technological problems.[53]

These practice management software applications, which run either on a desktop or on a server, combine legal research, billing programs, word processors, document management programs and other case management items (including "client and opposing counsel phone numbers, calendars, pleadings, discovery, and time-and billing information") in one centralized place.[54] This enables anyone in the firm, who is so authorized, to access clients' matters at a click of the mouse. Both legal online database services have products in this market. LexisNexis' practice management package is called Time Matters, whereas the Westlaw package is called Prolaw.

There is an additional concern with email communications over the prompt responsiveness to them. The MRPC 1.3 specifically provides that "a lawyer shall act with reasonable diligence and promptness in representing a client." Given the "virtual" reality of cyberspace, emails may not be perceived as real as phone calls or letters.[55] As a result, there may a tendency to procrastinate with the responsiveness of such correspondence. However, once email communications become part of the modes of communication with a firm, they are to be treated with the same diligence and promptness of all the other forms of communications used by that firm.

---

[52] Dennis Kennedy, Law Firms Play Catch-Up: Key Legal Technology Trends for 2002 (visited Jan. 10, 2002) http://www.llrx.com/features/techtrends2002.html.
[53] Id.
[54] Ashby Jones, Prolaw to the Rescue, New York Law Journal, Monday, February 4, 2002, vol. 227, no. 23, t4, col. 1.
[55] Lawson, Complete Internet Handbook, supra note 26, 206.

Internet Connectivity

1. Dial up Telephone Connections to Broadband

Originally, most people connected to the Internet via a telephone modem. Through the use of the modem, one's computer would be connected with a local ISP and that computer would be assigned with a temporary Internet Protocol (IP) address.[56] Once a connection was established, data retrieved from the Internet was transmitted in bites per second ("bps") and then loaded onto one's computer. The popular 1986 modem ran at 1200 bps (bites per second) compared to the present date "high end" modems of 56,600 bps.[57]

Today, Internet connectivity does not occur strictly through telephone modem dial ups, but rather through a number of ways through what is now coined as broadband Internet access. Broadband includes DSL, cable modems, ISDN or satellite dishes and T lines, which travel at anywhere from 56,000 bps to 45 Mbps.[58] The incredible speed and the growing affordability of broadband connectivity have greatly expanded the number of people turning to broadband. Moreover, with broadband connectivity, one can always remain connected to the Internet.

---

[56] Jim Calloway, Who is Reading Your Hard Drive Tonight? Security with High Speed Internet Access and a Few Words About Passwords (visited March 7, 2002) http://www.llrx.com/features/reading.htm.

[57] Internet Guide, supra note 10, 168.

[58] Internet Guide, supra note 10, 168. The Internet Guide gives the breakdown as follows: ISDN line (1B) 56,000 bps, ISDN line (2B) 128,000 bps, T-1 (high-capacity phone line 1.5 Mbps, T.V. cable (with special equipment) 4 to 10 Mbps, and T-3 (higher capacity phone line) 45 Mpbs.

Most law firms, regardless of size, now use DSL lines to access the Internet.[59] As prices have been significantly reduced for T1 service, other firms use T1 lines to connect, which to is believed to be a more stable and reliable than even DSL.[60] Some offices have the luxury of having both a both modes of Internet connectivity.

2. Security Issues

As noted, with broadband connections to the Internet, a firm can be constantly connected to the Internet. However, inherent in this is that while the firm is connected to Internet resources anywhere in the world, this connection to the Internet makes the computer and/or network vulnerable, as the connectivity is reciprocal.[61] In fact, the more continuous the connection is to the net, the greater the security risks. There are Internet "scanners" being used by people,

> who are sweeping the Internet looking SPECIFICALLY for computers running Windows File and Printer Sharing. And if those shares are password protected and sufficiently interesting, any freely available password cracker will silently pound on your password until your defenses have been penetrated.[62]

Security breaches can cause havoc including the introduction of viruses, the manipulation of data and the stealing of information. Measures to advert these dangers to a firm are necessary. Today, this is not a difficult thing to do, as firewall software is relatively inexpensive and easy to load on a computer, and if

---

[59] Sheryl L. Katz, Upgrade Your Firm's Internet Connection – Now! (visited March 7, 2002) http://www.llrx.com/extras/internetconnect.htm.
[60] Id.
[61] Steve Gibson, Internet Connection Security for Windows Users (visited March 7, 2002) http://grc.com/su-danger.htm.
[62] Id. Although Apple computers are vulnerable to such infiltration, they are designed with more built-in security features.

on a network, many routers now come with built-in firewall protection. The use of firewalls, although not foolproof, protects a computer or a network, as it provides a special filtering program between your computer or computers and the Internet.[63] This filtering software prevents unauthorized users from accessing one's system.

The most important security system, however, depends on the human component. Any sophisticated firewall system will fail to work if it is not properly configured or monitored. The proper use of passwords is another example. Passwords selected by firm members need to be changed periodically, they need to be unique, and they need to be kept secure. Proper and consistent vigilance to security matters is paramount to even the most sophisticated security computer system.

Cyberlegalethics

1. Avoiding the Unauthorized Practice of Law

Many firms are now putting their names out on the Internet via attorney directories, chat rooms, and Web sites. Site visitors sometimes seek and receive information or legal advice via these Internet sites.[64] Legal Web sites may have disclaimers for its site visitors, to avoid the appearance of establishing an attorney-client relationship with said visitors; however, these disclaimers are not sufficient protection. The ultimate test is what the visitor reasonably understood the relationship to be and, of course, this could be easily

[63] Lawson, Complete Internet Handbook, supra note 26, 426.

misconstrued, as there is a fine line between legal information and legal advice.

A firm's use of a Web site also raises the issue of unauthorized practice of law. DR 3-101(B) makes it improper for a lawyer to "practice law in a jurisdiction where to do so would be in violation of regulations of the profession in that jurisdiction." Some firms, in response, include disclaimers on their Web sites such as the following:

> This Web page is a public resource of general information available to all. It is intended, but not guaranteed or promised to be accurate, complete or current. This page is not intended to be an advertisement or legal solicitation, nor does it supply legal advice. The reader of this page should not consider the information given on this site to create an attorney-client relationship. The reader should not rely on the information provided herein and should always seek the advice of competent legal counsel in the jurisdiction or state the reader resides in.
>
> Furthermore, the owner or publisher of this site does not intend the links from this site to be an endorsement or referral, nor does he [she] guarantee or promise the accuracy of such links. The owner or publisher of this site shall not accept referrals from any unregistered referral service. In addition, the owner or publisher of this site does not wish to represent anyone who desires legal representation based upon the viewing of this site in their state of jurisdiction, if the site does not comply with all the laws and ethical rules of their state or jurisdiction.[65]

The Committee on Professional Ethics of the NYSBA, with its Opinion 709, also addressed the issue of the use of the Internet to advertise and to conduct law practice.[66] Although such activities were found to be permissible, the Committee held that firms engaging in these activities must comply with the NY Codes and Court Rules, and the rules of other jurisdictions, where possibly

---

[64] David A. Grossbaum, Casting Your Net For Clients, Using the Internet to Attract Clients Has Its Risk, ABA Network (visited Jan. 23, 2002) http://www.abanet.org/scripts/PrintView.asp.

[65] Internet York Guide, supra note 10, 153.

applicable. More specifically, the Committee held that legal practice on the Internet was “analogous to conducting a law practice by telephone or facsimile machine and is likewise permissible, subject to the same restrictions applicable to communication by those means.”

Notwithstanding the foregoing, the Committee addressed a few specific issues that extended to the Internet and needed to be met. For example, a firm, which posted in its law office "the Statement of Clients Rights and Responsibilities," as provided for in 22 N.Y.C.R.R. 1210.1, would be “prudent … to achieve substantial compliance with the terms of the rule (requiring posting of the Statement in the office in a manner visible to clients) by including the full text of the Statement on the attorneys web site.”

In turn, DR 5-105s and DR 5-108s, requires a firm to check for any possible conflicts of interest, also was addressed by the Committee. However, a conflicts check is not required when the rendering of “general information of an educational nature,” which does not include the obtaining of confidential information and there is no specific advice tailored to a client’s particular circumstances given.

a. Internet Advertising & Web sites

Many firms are advertising online. In fact, a firm web page, by itself may be considered a form of advertising or broadcasting.[67] Although there is debate about this issue, the consensus is that it is. If the web page is assumed to be a

---

[66] In Opinion 709, the firm in question had a trademark practice. Also, the Committee also examined the issue of the use of trade names.

[67] Internet Guide, supra note 10, 146.

form of advertising or broadcasting, then under DR 2-101(F), the "broadcast" is to be retained for not less than one year following transmission. Further, DR 2-101(A) prohibits the improper dissemination of deceptive or misleading information. Oftentimes the latter issue is raised with the use of links and frames.[68]

Under NYSBA Opinion 709, the Committee "believed that advertising via the Internet an electronic form of public media is permissible as long as the advertising is not false, deceptive or misleading, and otherwise adheres to the requirements set for in the Code."[69] The latter includes the retention for at least one year and possible filing of advertisements with the appropriate disciplinary committees.[70] And, if such advertising is intended to solicit clients outside of NYS, the advertisement "should inform a potential client of the jurisdiction in which the attorney is licensed, and should not mislead the potential client into believing that the attorney is licensed in a jurisdiction where the attorney is not licensed."[71] Furthermore, under DR 3-301(B), the firm may not render legal opinions over the Internet to clients outside of New York if such action constitutes the unauthorized practice of law in the other jurisdiction.

Generally, the Web site is considered passive in nature, hence not subjecting a firm to personal jurisdiction in a jurisdiction other than its own. However, given its commercial nature and its capability to provide for

---

[68] Id. at 151-52.
[69] DR 2-101, DR 2-102, EC 2-10.
[70] DR 2-101.
[71] See DR 2-102(D); the ABA Manual on Professional Conduct 81:551 (firm web pages should clearly identify the states in which they are licensed to practice)

interactivity, the Web site may subject a firm to personal jurisdiction in other states or foreign territories.[72] Given the "global availability of the Internet … makes it easy to 'practice law' in a jurisdiction where you are not licensed … If an online client does sue for legal advice given over the Web, you could be sued anywhere in the world."[73]

A Web site should only contain general public information. It should not give legal advice that may establish an unintended attorney-client relationship.[74] It must be clearly indicated that what is being given is legal information and not legal advice. In fact, one writer developed the following checklist:

> •Make it clear whether you are giving friendly advice or legal advice.
> •Do the same conflicts check you would do if the client came through the door.
> •Assume that the legal advice you give over the Internet is open to the public.
> •If you need to speak confidentially, use private email, telephone or letter.
> •Make sure that the legal Web site complies with the strictest advertising and fee splitting rules.
> •Indicate where you are licensed to practice and that you are not giving legal advice where you are not licensed to do so.
> •Buy worldwide malpractice coverage.[75]

Another writer suggested that a firm, engaged in Internet forums and/or maintaining a Web site, should integrate Internet communications with its normal conflict checking system.[76] In fact, the emails received from such Internet activity should be hyperlinked to go to a single email address, and the email can contain

---

[72] Internet Guide, supra note 10, 152-53.
[73] Grossbaum, supra note 60,
[74] Internet Guide, supra note 10, 152. The Guide also goes on to mention the risks involved in an attorney engaging in chat rooms or news group discussions.
[75] Grossbaum, supra note 60.
[76] Lawson, Complete Internet Handbook, supra note 26, 206.

a warning about email insecurity or provide encryption security.[77] This allows the firm to assign someone to properly check for any conflicts before a firm member is given the question to respond.

Moreover, firms should be cautious in not improperly engaging in solicitation over the Internet. Although solicitation is not allowed for in-person or on the telephone, it is allowed via "snail" mail. Hence, it is perceived allowed, by extension, via email.[78] Specifically, DR 2-101(F)(3) allows for targeted mail and maybe applicable to targeted email. However, in so doing, compliance with it requires the lawyer to retain the list of the people targeted for not less than one year of the last distribution. Further, under DR 2-101(K) requires that the document contain name, office address and telephone of the firm, and DR 2-101(F)(1), which requires the lawyer to meet the filing requirements within the state to which the targeted group were selected.

In order for a firm to protect itself, its Web site should also adhere to the guidelines, entitled Legal Websites Best Practice Guidelines, being developed by the Elawyering Task Force of the ABA Law Practice Management Section and ABA Standing Committee on the Delivery of Legal Services, latest draft approved for circulation for comment, dated October 15, 2001.[79]

First, the site should clearly identify the firm name, address, telephone numbers, and/or email address. This enables visitors of the site to ascertain the

---

[77] Id. at 206.
[78] Id. at 213-214.
[79] Legal Websites Best Practice Guidelines, ABA Network eLawyering (visited Jan. 10, 2002) http://www.elawyering.org/tools/practices.asp.

authority, ownership and authorship of the site. It also enables them to make contact with the firm, if needed or desired.

Second, the site should provide the date of the last revision. Given the changing face of the law, currency is critical. With the date of the last revision made available, the user may ascertain how to or not to rely on information that is available at the site.

Third, the site should clearly indicate the jurisdiction "to which any information relates."[80] This implicitly protects the firm from the appearance of unauthorized practice of law outside of its jurisdiction. And, explicitly, the visitor is made aware of the applicability or not of the information in his or her area.

Fourth, the site should provide a disclaimer, i.e., conspicuous notice that legal information on site does not constitute legal advice. The site should remind users about the limit of legal information in resolving legal problems."[81] Further, it is important to inform the visitors of the site the difference between legal information versus legal advice. A disclaimer is useful in this regard.[82]

Fifth, where appropriate, the site should provide links and annotation of other useful quality resources. This enables the user to collaborate and compare the information posted at the Web site with other sources. It also facilitates the visitor in finding additional information elsewhere.

Sixth, it should "provide links to relevant case law and legislation in correct form." Indicia of authenticity, accuracy and authorship should be

---

[80] Id.
[81] Id.
[82] See example of disclaimer supra.

standard fare to any materials posted on the Web site. Links to primary sources, legislation and case law should be provided to support the reliability of materials posted.

Seventh, "[w]here appropriate, the site should provide users with information on how and where to obtain legal advice or further information." This works together with guidelines three and four. Clarified should be the distinction between legal information obtained from the Web site versus legal advice that could only be properly obtained from lawyers who are licensed in the user's jurisdiction.

Eighth, the Web site host should have obtained all appropriate permissions to use any content from other providers and should acknowledge such sources on the site. This informs the user of the proper author of the information being relied because without such identification of source the user may mistakenly assume the frame and information therein belongs to the original site. Further, proper acknowledgement may also protect the Web site owner against any breaches of copyright.

Finally, the ninth and tenth guidelines recommend that the site clearly and conspicuously informs the users of the "terms and conditions" or "terms of service" to which they are authorized to use the Web site or to purchase products or services therefrom. In addition, the site should clearly disclose its policies on privacy and security of communications.

b. Extranets

Extranets are also becoming popular and are perceived as another way to securely and accurately exchange documents. Essentially, Extranets are private web sites restricted to either members of a group or select outsiders who have been given passwords.[83] The Extranet provider is in control of access and security.[84] These sites can serve as virtual data rooms or document repositories. The documents, being locally maintained and secured, are not subject to the transmission security issues. Authenticity of the documents is also assured. Clients, parties of a legal dispute, and law firm members can access posted documents 24 hours ad day, seven days a week, from anywhere.

During the litigation process, for example, firms can maintain files at their Extranets that include pleading files, document production, litigation calendars, deposition transcripts, witness lists, task lists and research materials.[85] Clients can check the status of their matters being handled by the firms. Negotiation status, litigation status and billing status can be maintained for clients to track. Resource materials, legal memoranda, key court cases and forms useful to clients can also be maintained.

Setting up an Extranet is not onerous. Some firms develop their own Extranet tools and others outsource it. Usually all that is required is Internet access and a web browser. The minimum security recommended is SSL for web

---

[83] Jerry Lawson, Law Firm Extranets: Baking a New Pie (visited March 7, 2002) http://www.netlawtools.com/nettools/extranets_legaltech.html

[84] Christopher King, Extranets Give Your Business an Edge, New York Law Journal, Monday, January 28, 2002, s13, col. 1.

[85] Id.

access.[86] Overall, an Extranet that is well designed requires little training for inputting data to it or to accessing the information from it. The authorized users are given a password, to which the users are entitled to access information posted at the Extranet site.

2. Verifying Information Found on the Web

In commenting on the duty under Canon 6 to "represent the client competently", the Committee stated that legal research for clients which "relies on information obtained from searching of Internet sites … requires that the attorney take care to assure that the information obtained is reliable." Digital signatures and encryption software will assist in assuring that transmitted documents and emails are authentic and have not been tampered with in transmission. However, documents found on the Internet when conducting research presents their own set of authentification and verification problems.

Other issues also arise, such as the reliability and accuracy of the information and the bias of the information found, as well as the timeliness of such documents. Further, once one has located a document, how long will it be kept on the site? The Internet is a treasure trove for current materials, but the archival of documents found is not, at present, one of its virtues as a research source.

The Internet provides legal researchers with a wealth of information. From any location where the Internet is available, a researcher may access databases, documents and sites for legal information. The Internet provides

---

[86] Id.

access to government and court documents, and current professional news and information. In addition, many paid subscription databases are now available on the Internet. LexisNexis and Westlaw no longer require direct dial in and special software to sign on to their respective databases. As long as one has a proper password and Internet access, those databases are available.

The growth of the Internet and the ease with which information may be made available through it has resulted in a lot of Web sites offering legal information. However, before retrieving materials from the Internet, those materials must be scrutinized. Although paid subscription databases such as LexisNexis and Westlaw may also have inaccurate documents on their databases; their business is contingent on the trust its clients have in the contents of their database, as well as the currency. Their material is thoroughly evaluated for its content, authorship and authenticity. Plus both services archive a lot of materials. Freely available Internet sites many not keep to the same high standards.

When obtaining documents from free sites, one must subject the materials and the sites from where they are retrieved to greater scrutiny. As one source noted, "[t]he Internet epitomizes the concept of *caveat lector: Let the reader beware*."[87] Having said this, there are a number of criteria, which should be used to evaluate documents and information found on the Internet. A quick checklist

---

[87] Evaluating Information Found on the Internet (visited March 4, 2002) http://www.library.jhu.edu/elp/useit/evaluate/index.html.

for evaluating an Internet document, offered by a web manager at a law firm Web site, is:[88]

1. Determine its origin. Discover the author AND the publisher.
2. Ascertain the author and publisher's credentials.
3. Discover the date of the writing. This gives the information historical context.
4. Verify it. Find another reputable source that provides similar information.

Dissecting this further, starting with the issue of authorship, one should look for the author of the document. Is there an author noted? Who is the author? What credentials are available about the author at the site? Is there information given about the author, including contact information? Is the author affiliated with an organization? In fact, one can also search the author's name on an Internet search engine or in other databases to obtain further information about the person's identity and affiliations.[89]

Although most information is subjective, one must also closely examine a document in terms of its bias. Sometimes ascertaining its source and the Web site from whence it was retrieved may answer that question. For example, if the document was found at a commercial site, it may be geared at presenting that company, its products, etc., in a positive light. In addition, the document may also be trying to promote or advertise a service, a product, a cause, etc.

A research document usually carries indicia of credibility. Information, such as bibliographic references and acknowledgements, is standard fare and

---

[88] Genie Tyburski. Assess the Quality of Information at a Web Site (visited March 4, 2002) http://www.virtualchase.com/howto/assess_quality.html.

[89] Practical Steps in Evaluating Internet Resources (visited March 4, 2002) http://www.library.jhu.edu/elp/useit/evaluate/practical.html.

should appear. The document may also explain the research methods used to gather information and interpret it.[90] Time should be taken to confirm the completeness and accuracy of the document.

Further, one should look at the timeliness of the document. This information as to the currency of the document may be ascertained by looking for a copyright date and the date in which the document and/or the site was last updated. In addition, other indicia of currency include internal confirmation, e.g., "Based on the 1990 US Census data" or "Closing stock prices, September 30, 1996."[91]

Next, the publishing body should be scrutinized. What type of site is it? What credentials are available about the site? Look at the domain address, is the site commercial (.com or .net), academic (.edu), government (.gov), nonprofit (.org), military (.mil) etc.[92] What is the overall look of the site, i.e., its design, organization, navigation (including search engines), contents (including any archival features), links and contact information.[93] Does it clearly provide information about the site's ownership, targeted users, its mission and its Web site's currency?[94] How comprehensive is the site? Do other Internet sites link to this site?

---

[90] Elizabeth E. Kirk, Evaluating Information Found on the Internet (visited March 4, 2002) http://wwwlibrary.jhu.edu/elp/useit/evaluate/index.html.
[91] Practical Steps, supra note 86.
[92] E.g., a domain name of .info is for corporate information, and a site sponsored by a country is indicated by two letter country identifications, such as .uk for the United Kingdom.
[93] Sabrina I. Pacifici, Getting it Right: Verifying Sources on the Net (visited March 4, 2002) http://www.llrx.com/features/verifying.htm.
[94] Id.

In fact, domain registration information may be obtained about the site. This information is public for most sites (however, some legitimate sites may elect to keep this information anonymous). The following are sites that provide that information for free:[95]

VeriSign -- www.netsol.com/cgi-bin/whois/whois
ARIN -- www.arin.net/whois
InterNic – www.internic.net/whois.html
SamSpade.org – www.samspade.org

These sites provide information about the queried site such as the name, address, telephone number, domain server data and registration date.

Certain sites such as those maintained by government and academic institutions confer, by their very nature, a higher level of trust. Other examples of sites that are afforded a similar high level of trust are Web sites such as those owned by well recognized news, media and other organizations,[96] such as CNN, the New York Times; and law specific, the New York Law Journal, ABA, LexisNexis and Westlaw. The information posted at these types of sites may also contain inaccuracies, biases and the like, but overall the concerns about verification and authenticity are greatly reduced.

[95] Id.
[96] Id.