NFPA Informal Ethics and Disciplinary Opinion No. 96-1

The following ethics and disciplinary opinion of the National Federation of Paralegal Associations (NFPA) is offered based upon its positions and research in the area of paralegal ethics. It should not be construed as binding and must be interpreted in conjunction with the applicable state's Supreme Court rules and opinions governing the professional conduct of members of the legal profession. This opinion may be used for guidance and, by the appropriate entity, as a persuasive argument in favor of the findings of NFPA.

Question: ***What are the ethical implications concerning client confidentiality, if any, of paralegals communicating in cyberspace?***

Facts: The National Federation of Paralegal Associations, Inc. (NFPA) was the first national legal organization to establish a presence on the World Wide Web at http://backup.paralegals.org. In the earliest stages of developing resources and benefits available to NFPA members through this presence in cyberspace, the NFPA Ethics Board identified several ethical dilemmas which could be faced by paralegals in several forums for cybercommunications. Consequently, to continue its commitment to providing paralegals with information and resources to assist to maintain appropriate professional conduct, the NFPA Ethics Board issues this opinion with respect to maintaining client confidentiality in cyberspace.

Opinion: Paralegals communicating in cyberspace through any form of electronic communication shall maintain and preserve client confidences and secrets. Electronic communications may include, but are not limited to, communications transmitted or posted through E-mail (electronic mail), list serves, bulletin boards, World Wide Web forums, forums and mailings and other public or semi-public forums located at websites, Internet Relay Chats, usenets and newsgroups.

Discussion: The economic advantages derived from conducting research, investigation and communications in cyberspace are becoming widely known within the legal and business communities. At a time when clients are concerned about the delivery of cost-effective legal services, attorneys and paralegals are able to provide clients with a higher caliber work product at a lower cost and/or more efficiently through the use of computer technology and the Internet.[*1]

Recognizing its role to provide resources and benefits to its members as well as information about the paralegal profession to legal professionals and consumers, the National Federation of Paralegal Associations, Inc. (NFPA) became the first national legal organization to establish a presence on the World Wide Web at http://backup.paralegals.org. One of NFPA's earliest activities in this regard was to develop list serves (also known as list services), a method for individuals to communicate through sending an e-mail message to anyone registered for the list and to receive public and private responses to the message.

NFPA's list serves were developed to enable its members to communicate with each other about topics relevant to paralegals. The NFPA Board of Directors determined that the list serves would not be moderated or censored in any formal way so that registrants would be able to freely communicate about topics of their choice.*2

In the earliest stages of developing resources and benefits available to NFPA members through this presence in cyberspace, the NFPA Ethics Board identified several ethical dilemmas which could be faced by paralegals in several forums for cybercommunications. In particular, the NFPA Ethics Board noted that one or more messages being transmitted by registrant(s) might present a problem with maintaining client confidentiality and privilege. Accordingly, to continue its commitment to providing paralegals with information and resources to assist to maintain appropriate professional conduct, the NFPA Ethics Board created a guideline which is sent to each new subscriber to the list serve. It reads,

> *Electronic communications, specifically including e-mails and list serve messages transmitted via e-mail, are not confidential. Therefore, confidential and/or privileged information shall not be transmitted via any subscriber to these list serves.* Confidential information *for the purposes of e-mail and list serve communications, also includes a client or party's name, or other information relating to a client or the client's legal matter which could identify the client or client's legal matter, whatever its source. For further information, please see NFPA Model Code of Ethics and Responsibility, Canon 5 and ethical considerations thereto or request additional information by sending an e-mail to* nfpa-info@paralegals.org.

However, the NFPA Ethics Board recognized that this standard of maintaining and preserving client confidentiality needed to be imposed on all cybercommunications since existing ethics rules and regulations do not yet adequately address the unique issues raised by the Internet.*4 *5

NFPA addresses a paralegal's ethical responsibility to maintain client confidentiality in its Model Code of Ethics and Responsibility (Model Code) at Canon 5 and ethical considerations thereto, incorporated herein as though set forth at length. Canon 5 of the Model Code states that, *a paralegal shall preserve all confidential information provided by the client or acquired from other sources before, during, and after the course of the professional relationship.* Naturally, these obligations are derived from the Rules of Professional Conduct and Code of Professional Responsibility governing attorneys with respect to client confidences and secrets. *6 NFPA interprets this ethical obligation to extend to any form of communication, including electronic communication in cyberspace, *e.g.*, e-mail, list serves, bulletin boards, World Wide Web forms, forums and mailings, Internet Relay Chats, usenets and/or newsgroups.

This belief is supported by the American Bar Association Standing Committee on Lawyers' Responsibility for Client Protection, albeit over ten years old and a broad and

general recommendation at best. In its report, the Committee suggested that a lawyer should not communicate over an on-line network regarding confidential matters without being assured, *either through bar approval or through the lawyer's own informed evaluation*, of the reliability of the system operator in maintaining confidential information. *7 The Committee also said that a lawyer should not communicate over an on-line network regarding confidential matters *without being reasonably assured of the security of the system and protection from the inadvertent or intentional interception of information by another.* *8 Demonstrating the ABA's concern over maintaining client confidentiality when computers are used in the practice of law, the ABA recently issued a formal opinion on a more narrow subject stating that a law firm may allow a computer maintenance company or other service provider access to the firm's client files, but must make reasonable efforts, such as a written confidentiality agreement, to ensure that the company will not disclose any of the files' content. *9

While several bar associations are investigating the issues concerning confidentiality and privilege in cyberspace, few have issued formal opinions directly on point; most are dealing with attorney advertising, solicitation and related issues first, *e.g.*, Pennsylvania, Georgia, Texas, California, New Jersey. Those which have discussed confidential communications analogize Internet communications to those issued with respect to cellular phone communication. *10 For example, South Carolina Ethics Opinion 94-27 states that *without certainty that electronic lawyer-client communications remain confidential, representation of or communication with a client via on-line electronic media may violate Rule 1.6 absent an express waiver by the client.* *11 South Carolina also distinguished private electronic mail from public notices on electronic bulletin boards but stated *the very nature of on-line services makes it possible for their system operators to gain access to all communications that are transmitted through them.* *12 In addition, Iowa has issued an advisory opinion suggesting that communications with clients must be encrypted, and Arizona has issued an informal, non-binding statement that confidential material sent via e-mail should be encrypted to avoid breaching the duty of confidentiality. *13 *14

Another important consideration with respect to paralegal cybercommunications is preserving client privileges, not necessarily addressed by the Rules of Professional Responsibility or Code of Professional Conduct. *15 However, a lot of the law with respect to privilege in cyberspace originates in criminal cases. This belief would be supported by the precedent-setting Sixth Circuit decision in *U.S. v. Thomas*, 74 F.3d 701, 1996 U.S. App. Lexis 1069 (6th Cir. 1996), *cert. pending* which applied federal communications laws concerning interstate commerce via electrical transmission to computer files traveling via modem through cyberspace. *16 *17

Originating in the Wiretap Act, and amended by the Electronic Communications Privacy Act, 18 U.S.C.A. 2510, *et seq.* (1988), reading (also referred to as intercepting and/or disclosing) electronic mail messages exchanged over public e-mail systems by anyone other than the sender and receiver is a felony. Presumably, the attorney-client privilege and, hence, the paralegal-client privilege, would be preserved according to 2517(4) which provides that *no otherwise privileged wire, oral or electronic communication intercepted*

in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character. However, some would argue that the jury is still out on the attorney-client privilege extending to paralegals and in all forms of cybercommunications because of the lack of determination that an Internet user has a reasonable expectation of privacy. *18 Debate continues over whether unencrypted e-mail can be presumed secure. With the exception of *U.S. v. Maxwell*, no court has directly addressed whether encrypted mail preserves the privilege and confidentiality of client communications.

Even if the author carefully prepares an electronic communication, it is possible, albeit illegal, to intercept that communication. It is also possible for electronic communications to be delivered to an unintended party inadvertently. The question yet to be resolved by the courts is whether the disclosure or waiver was inadvertent or intended. Importantly, with the proliferation of a variety of computer criminals, *e.g.*, hackers, crackers, sniffers and spoofers, communicating in cyberspace leaves open a myriad of potential other means to inadvertently disclose and/or purposefully retrieve confidential information by other individuals and entities. Accordingly, proper security measures should be evaluated by any legal professional to ensure that e-mail messages are not intercepted, altered or otherwise misused.

One form of security is encryption, however, there is no definite evidence that it will secure all Internet communications; in addition, encryption presents other problems as well, *e.g.*, administration, distribution and authentication. *19 Some attorneys and bar organizations have suggested, but not yet imposed an obligation to encrypt e-mail communications concerning clients. In fact, numerous cyberlegalethics experts disagree that encryption solves the potential problems associated with cyberspace let alone that it is necessary to preserve client confidentiality and privilege. *20 In fact, the Attorneys' Liability Assurance Society (ALAS), a law firm malpractice insurance company, states that it is not necessary for ethics, privilege or liability purposes to encrypt communications on the Internet except for matters so important that *any* threat of interception must be avoided. *21

Another form of security or attempt to preserve the confidential nature of communications is to add a disclaimer. Many law firms and legal departments of corporations have done so. For instance, with respect to client e-mail communication, some have suggested the following disclaimer:

> *E-mail communication on the Internet may NOT be secure. There is a risk that this confidential communication may be intercepted illegally. There may also be a risk of waiving attorney-client and/or work-product privileges that may attach to this communication. DO NOT forward this message to any third party. If you have any questions regarding this notice, please contact the sender.* *22

With respect to inadvertent disclosure, in pertinent part,

> *DO NOT read, copy or disseminate this communication unless you are the intended addressee. This e-mail communication contains confidential and/or privileged information intended only for the addressee. If you have received this communication in error, please call us (collect) immediately at [insert phone number] and speak to the sender of the communication. Also, please notify immediately via e-mail the sender that you have received the communication in error.* *23

To date, the courts have ruled that there is a reasonable expectation of privacy in private e-mails. *24 However, the Internet *inter alia* has been determined to be a public medium in a case challenging the Texas State Bar Association's rules limiting lawyers' advertising activities in the public media. *25 In fact, an opinion concerning a securities fraud action included dicta that the *information superhighway* is a source of information in the public domain. *26 Hence, such a conclusion about privacy of e-mails cannot be drawn on list serves and certainly does not exist in other forms of public or quasi-public communications, which, in some cases, are searchable using a variety of Internet search engines. If the information communicated is not private then, a breach of client confidentiality or privilege may arise. In *Castano v. American Tobacco Company*, 896 F. Supp. 590 (E.D.La. 1995), the court refused to suppress allegedly privileged documents that defendants had made publicly available on the Internet, but reserved the question whether use of such documents in discovery or at trial might be prohibited.

The risks of communicating over the Internet are summarized as follows:

- the lack of a final judicial determination about the confidentiality and privilege;
- the possibility that confidential communications may be retained and subject to discovery or inadvertent disclosure;
- that inadvertent disclosure may occur because of the way information is transmitted within the Internet; and
- the risk that the communication may be construed to be consent to disclosure and thus, waivers of confidentiality. *27

As a result of these potential risks, legal professionals should take appropriate steps to ensure internal security within a law office or legal department with respect to access to computer terminals and passwords, etc. Legal professionals should also establish procedures and/or policies to ensure that confidentiality is protected in public or quasi-public posts. Additionally, encryption techniques may be considered as a means to protect the confidentiality of communications.

Albeit laden with unresolved disputes concerning client confidentiality and privilege, NFPA still strongly believes that cyberspace presents extraordinary opportunities to conduct paralegal work in a cost-efficient manner benefiting both the legal profession and public it serves. In the absence of methods to secure undeniably Internet communications

and of regulations governing those communications, NFPA believes that the same standards which govern other communications, govern those conducted by and engaged in by paralegals in cyberspace. By NFPA recognizing a paralegal's ethical obligations in cyberspace, NFPA continues to recognize the profession's responsibilities to the public, the legal community and colleagues.

NFPA's Model Code of Ethics and Professional Responsibility and positions on issues affecting the paralegal profession have been designed to provide paralegals with information and direction concerning various ethical issues which arise in their careers. It is important that paralegals realize and understand their obligations to the attorney and the client so that the client receives both high caliber and cost efficient legal services.

Indemnification of NFPA: By making a request to the National Federation of Paralegal Associations for an opinion and/or recommendation concerning proper conduct for a member of the legal profession as it pertains to ethical conduct, obligations, utilization and/or discipline of paralegals, the inquirer and his/her employers, employees, agents, and representatives agree to indemnify, hold harmless, and defend the NFPA, its Officers, Directors, Coordinators, Ethics Board and Managing Director from any claims arising from any act or omission of NFPA except those occasioned by NFPA's willful or deliberate acts.

---

*1 The *Internet* as used herein includes any form of cyberspace communication including, but not limited to, those collectively referred to as the World Wide Web and the Information Superhighway.

*2 However, list serve participation may be withdrawn for bringing topics not related to paralegals and their profession, using profanity, verbally attacking or slandering another or using the list serve to solicit business by wholesale mass marketing.

*3 "About Legalethics.com" (The Practicing Attorney's Home Page), *http://www.legalethics.com/info.htm,* Internet Legal Services (1996).

*4 *Cyberlegalethics* refers to ethical rules governing conduct of legal professionals in cyberspace.

*5 *See also*, Kligerman, S.D., *Cyberlegalethics ... Cyber* Who *???*, *National Paralegal Reporter,* (Summer, 1997).

*6 American Bar Association Model Rule of Professional Conduct 1.6 and Model Code of Professional Responsibility DR 4-101.

*7 Rogers, J.C., *Analysis: Ethical and Malpractice Concerns Cloud E-Mail, On-Line Advice*, http://www.bna.com/hub/bna/legal/adnew2.html, *ABA/BNA Lawyers' Manual on Professional Conduct* (1996), citing ABA Standing Committee on Lawyers Professional

Responsibility for Client Protection, *Lawyers on Line: Ethical Perspectives in the Use of Telecomputer Communication* (1986) at 67.

*8 *Ibid.*

*9 American Bar Association Formal Ethics Opinion 95-398, *Law.Man.Prof. Conduct 1001:316* (1995).

*10 *E.g.*, Massachusetts Ethics Opinion 94-5 (1994); New York City Ethics Opinion 1994-11; New Hampshire Ethics Opinion 1991-92/6 (1992). Reference to these opinions is not intended to suggest that the NFPA Ethics Board necessarily adopts the analogy. Indeed, the Board notes that many of these opinions were issued prior to legislation which makes it illegal to intercept certain electronic communications. *See*, Wiretap Act, and amended by the Electronic Communications Privacy Act, 18 U.S.C.A. 2510, *et seq.* (1988).

*11 South Carolina Ethics Opinion 94-27, 11 Law.Man.Prof. Conduct 67 (1995) cited at Rogers, J.C., *Analysis: Ethical and Malpractice Concerns Cloud E-Mail, On-Line Advice*, http://www.bna.com/hub/bna/legal/adnew2.html, *ABA/BNA Lawyers' Manual on Professional Conduct* (1996).

*12 *Ibid.*

*13 Iowa Advisory Opinion No. 95-30, [citation omitted] (1995).

*14 Ross, S.B., *E-mail: How Attorneys Are Changing the Way They Communicate* (Jul. 19, 1996).

*15 Rogers, J.C., *Analysis: Ethical and Malpractice Concerns Cloud E-Mail, On-Line Advice*, http://www.bna.com/hub/bna/legal/adnew2.html, *ABA/BNA Lawyers' Manual on Professional Conduct* (1996).

*16 *The Cyberlaw Practitioner*, http://www.gse.ucla.edu/lclp/feb96.html, The UCLA Online Institute for Cyberspace Law and Policy, citing Biegel, S., *Constitutional Issues in Cyberspace Focus on 'Community Standards,' Los Angeles Daily Journal* (Feb. 22, 1996).,

*17 *See also, U.S. v. Gilboe*, 684 F.2d 235 (2d Cir. 1982), *cert. denied*, 459 U.S. 1201 (1983) in which the defense argument that an electronic transfer was not *transportation* was rejected in a matter involving a conviction for transportation of money obtained by fraud; the California Business and Professions Code 6157 and 6158 referring to *electronic media* which is defined to include *computer networks*.

*18 *See e.g.*, Rogers, J.C., *Analysis: Ethical and Malpractice Concerns Cloud E-Mail, On-Line Advice*, http://www.bna.com/hub/bna/legal/adnew2.html, *ABA/BNA Lawyers' Manual on Professional Conduct* (1996), citing results of informal and unscientific

survey posted on Net-Lawyers list serve at http://www.webcom.com/~lewrose/netlawyers/ (Jan. 26, 1996).

*19 Bruce Schneier, *E-Mail Security* 41 (1995), cited at The Lawyer's Privacy Problems with Internet E-Mail, *http://www.computerbar.org/netethics/bjones.htm#fn20*. *See also*, Lawson, J., *An Encryption Primer for Attorneys* included in *Lawyers on Line: A Guide to Using the Internet*, Virginia Continuing Legal Education (1995), also available at lawson@sblegal.com; http://www.sblegal.com/sunburst/.

*20 *E.g., ALAS [Attorneys' Liability Assurance Society, Inc.] Loss Prevention Manual, Tab III.C,* however noting that the author takes the position that attorneys should use caution, cited at "Issues:Legalethics.com" (The Practicing Attorney's Home Page), *http://www.legalethics.com/Issues.htm*, Internet Legal Services (1996).

*21 Freivogel, W. *Communicating with or About Clients on the Internet: Legal, Ethical, and Liability Concerns*, *ALAS Loss Prevention J.* 17, 19 (Jan. 1996).

*22 Krakaur, P., *Blasting Off Into Cyberspace -- Surfing the Net's Ethical Issues, Three Draft Disclaimers*, "The Second Annual Statewide Ethics Symposium of the State Bar of California Committee on Professional Responsibility and Conduct" (May 11, 1996). [Disclaimers at http://www.legalethics.com/draft.htm incorporated herein as though set forth at length; for discussion, educational and informational purposes only.]

*23 *Ibid.*

*24 *See, U.S. v. Maxwell*, 42 M.J. 568 (US Air Force CtCrimApp 1995), as to application of Fourth Amendment search and seizure purposes.

*25 *Texans against Censorship, Inc. v. State Bar of Texas*, 888 F. Supp. 1328 (E.D. Tex. 1995).

*26 *Whirlpool Financial Corp. v. GN Holdings, Inc.*, 67 F.3d 605 (7th Cir. 1995). [Interestingly, but a matter reserved for later discussion, the court held also that since the reasonable investor is presumed to have information in the public domain, and that the *information superhighway* is a source of such information, a duty to investigate the resources on the Internet exists.]

*27 Lanctot, C.J. and Maule, J.E., *The Internet -- Hip or Hype? Legal Ethics and the Internet*, http://www.law.vill.edu/vcilp/MacCrate/mcle/lanctot.htm#confidentiality, Villanova University Law School (19).

Issued: December 30, 1996.