Gary L Stuart
Lexis.Nexis Exchange
Published Article—September 1997

E-Mail and E.R. 1.6

The single most difficult ethical challenge for the lawyer who communicates with clients or potential clients over the Internet is confidentiality. There are a wide variety of potential eavesdroppers on the Internet. The electronic age has brought with it new names for people who casually or intentionally pry into the electronic affairs of others. These include: Hackers, Crackers, Spoofers and Sniffers.

A "hacker" is intensely interested in complex computer systems. But, much to the dismay of the so-called "legitimate" hacker, the term has also become synonymous with "cracker"—one whose interest includes unauthorized entry and modification of these computer systems. Legitimate hackers are often system operators and administrators who detect, repair and prevent the break-in and damage by crackers.

Coming across a file or document that seems interesting, a cracker can copy it, alter it, delete it, or read it. Crackers can create ethical problems for the lawyer who, although connected to a network, does not communicate by e-mail. The technology to crack not only e-mail, but also private internal files is now widely available. Recently, a tool for probing a remote computer for security vulnerabilities became available. This is Security Administrator Tool for Analyzing Networks (SATAN). SATAN not only analyzes the remote computer's weak points, but it also provides extensive documentation on the vulnerabilities identified and how to repair them.

SATAN was not the first computer program to be used by crackers but it is dangerous because it has been released to the Internet. This means it is widely available for both legitimate use by system administrators and unethical use by crackers. In the offices of some law firms there is a race between the system administrators to find and plug the leaks in their computers' security and the crackers intent on finding and exploiting those weaknesses. The lawyer that assumes the problem is fixed by providing a simple electronic means of protecting e-mail is walking on thin ethical ice.

If the computer that originates and receives e-mail is left open for exploration via a network outside the firm, the problem is not "fixed" by an electronic password. More complex measures are often called for. These may include public key encryption, digital signatures and sophisticated access codes frequently changed. Sharing of communications lines means that computers can receive information actually intended for other computers on the network. Capturing this information as it is going over the network is called "sniffing." Sniffers have the potential to create ethical dilemmas that the lawyer of just a few years ago could not have even imagined, much less understood.

One common way of connecting computers is through an Ethernet. This works by transmitting data in "packets" to all of the computers on the same circuit. Each packet begins with a "header." The header contains the address of the sender, the address of the recipient, and other

information required to keep the communications organized and reliable. The message itself follows the header.

Unless encryption is used, the message data is transmitted as text just as it would normally be displayed on the recipient's screen. Optimally, computers on the network will only accept the packets addressed to them. Unfortunately, for the unwary lawyer, "sniffer" software is easily obtained. When loaded onto a computer on the network this software will accept the data regardless of what the packet header indicates the intended recipient to be.

Extended data (such as long pleadings or discovery documents) may occupy many data packets, but the technique is the same regardless of message length. The data from the packets stored on the sniffer's computer can be reassembled into a single contiguous block of data.

The most insidious ethical challenge presented by the sniffer is that they do not have to know your password to steal your client's secrets, your litigation strategy, the jury consultant's analysis of potential jurors, or your cost ledger on the file. Once the data is transmitted onto the Internet, it becomes fair game.

Computer sniffing is a violation of law. It is the subject of several federal statues and state codes. While those laws do not relieve the lawyer of the duty to protect the secrets and confidences of the client, they are worth reviewing as part of the ethical analysis of any computer package or system used to communicate with clients.

Under the Electronic Communications Privacy Act ("ECPA"),[1] reading electronic mail messages exchanged over public e-mail systems by anyone other than the sender and receiver is a felony. For purposes ethical analysis, the Internet must be considered a public e-mail system even if you have password protection with your Internet Service Provider.

Unencrypted e-mail messages are an unnecessary temptation to these legitimate sniffers. Just as some people occasionally pretend to be someone they are not, so do computers. This is called "spoofing." Whereas sniffers use data packet headers, spoofers use the recipient address. Once that is obtained, the spoofer computer configures itself to emulate the recipient's machine. When data comes along the network intended for the actual recipient, the spoofer receives it instead. Some spoofer programs automatically send a packet to the sender which makes the sender believe that the message was properly received. This allows the spoofer computer to read the e-mail, make up a reply and send it back to the unsuspecting lawyer who is unaware that he is communicating with an impostor.

Even absent hacking, cracking, sniffing or spoofing, it is possible for someone to gain access to a lawyer's password. Once that security is breached, the lawyer's computer can send out inauthentic messages.

Client confidentiality and privacy can be compromised by the weakest application in the computer-chain. If co-counsel, support staff, consultants, or others have physical access to the lawyer's computer, or password, even public key encryption and digital signatures may be inadequate.

[1] 18 U.S.C.A 2510, et. seq. (1988).

The answers to these ethical dilemmas include proper physical security measures, staff screenings, firewalls, digital signatures, encryption, secure-socket layer technology, common sense and heightened security when communicating electronically.

Lawyers must understand that Internet e-mail is not the same as the firm's internal e-mail system because it is not transmitted over a secured network. Technologically and analytically, Internet e-mail may be safely sent without encryption; however, it may be ethically unwise to do so.

The concern over clear-text e-mail was noted in a recent federal case in which the judge declared that the client's claim of privilege was lost when the documents were sent to the client in clear text and were available through a state library on the Internet. The court held that the documents were in the public domain.[2]

Encryption of e-mail, while both necessary and desirable, will not cure all the ethical problems associated with e-mail security. But, if the lawyer makes encryption a major part of the physical, operational, and computer security planning, it can substantially ensure that client e-mail messages will not be overheard, intercepted, altered or otherwise misused while in transit over a network (private or public) or while they are resident on some computer database or hard-drive.

It must be emphasized there is no clear consensus or body of law to establish the ethical necessity of encryption of Internet e-mail. From an ethical standpoint, the central issue is the effectiveness of the lawyer's encryption software in communicating with clients via e-mail over unsecured networks. The practical issues include administration, distribution, and authentication of a multitude of users' encryption keys. That is not a small matter. Consequently it can become an ethical matter since the cost of the system can either be absorbed or passed on to the client.

Robust encryption can virtually guarantee that sniffers cannot read the data in the packets that they "hear." The text is so garbled that it is unintelligible. Spoofers are equally frustrated by encryption. Even where the message itself is not encrypted, i.e., it is transmitted in clear text, encryption can provide substantial certainty that any message received was transmitted by the individual purporting to have sent it. Sophisticated encryption software can even scramble the packet header information so it is impractical to spoof the message.

In mid-1996, a standard was proposed against which encryption software would conform. It is called Privacy Enhanced Mail (PEM). It may be the solution for both privacy issues and industry standardization. It is important to the lawyer because it is vital that clients know that the person with whom they are communicating is the lawyer and not an impostor. In addition to ease of use and robust encryption, PEM has the capability of electronically "signing" e-mail messages such that one's signature is capable of accurate authentication. This makes it far more likely that the message came from the purported sender.

Electronically Privileged E-Mail

ABA Model Rule 1.6 precludes a lawyer from disclosing "information relating to representing of a client unless the client consents after consultation.[3] DR 4-101 of the ABA Model Code prohibits the lawyer from "knowingly" revealing information protected by the attorney client

[2]Castano v. American Tobacco Co. 896 F. Supp. 590 (D.C. Est. La. 1995).

[3]MODEL RULES OF PROFESSIONAL CONDUCT 1.6.

privilege and other information gained in the professional relationship that might embarrass or be detrimental to the client or that the client wants to remain secret.

Several state bar ethics committees have considered the confidentiality question. Since there is no certainty that electronic lawyer-client communications remain confidential on-line, some have ruled communications with a client on-line violate ABA Model Rule 1.6, absent an express waiver from the client.[4]

The Iowa Supreme Court Ethics Board recently rescinded a controversial opinion regarding encryption of e-mail for client sensitive material. The opinion allows Iowa lawyers to send clear text e-mail to clients over the Internet "if they obtain informed consent and acknowledgment of the risks."[5] This must be done in writing. Absent that acknowledgment, lawyers must encrypt the material or otherwise protect it by a password/firewall or some accepted equivalent security system.[6] Three additional states have essentially approved the use of Internet e-mail without encryption, except for highly sensitive information.[7]

The traditional approach to the attorney-client privilege is complicated enough in the world of paper and oral communications. It becomes more so in the world of electronic communications, in part, because of the problem of inadvertent eavesdropping.

Courts, lawyers and clients all agree that reasonable precautions must protect and preserve client confidentiality. If reasonable precautions are taken, and unbeknownst to either the lawyer or the client, electronic eavesdropping occurs, it will not cause the privilege to be waived.

In ruling on whether an inadvertent disclosure waives the privilege, courts typically consider the circumstances surrounding a disclosure on an *ad hoc* basis.[8] An *ad hoc* analysis serves the purpose of the attorney-client privilege, which is the protection of the communications that clients intend to remain confidential, but permits those claiming the privilege to feel "the consequences of their carelessness if the circumstances surrounding the disclosure do not clearly demonstrate that continued protection is warranted.[9]

The first test in any such *ad hoc* analysis is whether the precautions taken by the lawyer and the client were reasonable, that is, were they designed to prevent inadvertent disclosure. Although waivers must typically be intentional or knowing acts, inadvertent disclosures are, by definition, unintentional acts. Consequently, disclosures may occur under circumstances of such extreme or gross negligence as to warrant deeming the act of disclosure to be intentional.[10]

Lawyers communicating electronically over an unsecured network (such as the Internet) rely on encryption the same way the paper lawyer relies on sealed envelopes and secure delivery systems.

---

[4]*See generally*, South Carolina Ethics Opinion 94-27; Massachusetts Ethics Opinion 94-5; New York City Ethics Opinion 1994-11 (1994); New Hampshire Ethics Opinion 1991-92/6 (1992).

[5]Iowa Supreme Court Ethics Board Opinion 95-30 (May 18, 1996) as reported in ABA/BNA Lawyers' Manual on Professional Conduct, Vol. 12, No. 17, Sep. 18, 1996.

[6]*Id.*

[7] Arizona Ethics Opinion 97-4 (April, 1997); Vermont Bar Association Committee on Professional Responsibility, Opinion 97-5; District of Columbia Bar Legal Ethics Committee, Opinion 272 (May, 1997).

[8]Alldread v. City of Grenada, 988 F.2d 1425 (5th Cir. 1993).

[9]*Id.*

[10]F.D.I.C. v. Marine Midland Realty Corp. 138 F.R.D. 479 (E.D. Va. 1991).

Encryption for messages in transit functions in the same way sealed envelopes do in furthering the reasonableness of the expectation that the contents will remain private. Just as there is a substantial nexus between the use of seals on envelopes and the client's expectation of privacy in paper communications, so too is there a nexus between encryption and the expectation of privacy in e-mail over the Internet.

This substantial nexus solidifies the reasonableness of the expectation that the communication was intended to remain confidential because of the extra effort put forth to encrypt it. As of mid-1997, there do not appear to be any appellate decisions addressing the specific question of whether transmission of clear-text "confidential" messages over the Internet is an intentional divulgence of that information. Consequently there can be no clear answer to the related question of waiver by the client.

The closest analogy is a U. S. District Court case where the court held that the interception of a mobile telephone conversation between a lawyer and a client did not violate the ECPA.[11] The court held there is no reasonable expectation of privacy in a communication broadcast by radio in all directions and which could be overheard by countless people. That case did not involve an analysis of waiver of the attorney-client privilege because the opposing counsel, the prosecutor, did not attempt to use the intercepted information as evidence. The issue was presented to the trial judge in a private action under the ECPA.[12]

Password security (as opposed to encryption) was the subject of the court's holding in a recent online e-mail case.[13] The case was tried in a military court which did not directly address whether unencrypted e-mail meets the requirement that lawyer-client communications be conducted outside the presence of strangers to remain confidential. The court discussed the expectation of privacy in e-mail messages for Fourth Amendment search and seizure purposes. The court held that the sender of an e-mail message had an objective expectation of privacy regarding messages to other subscribers of a private online service (America Online). All subscribers had been individually assigned passwords. The court noted there "was virtually no risk that. . . computer communications would be received by anyone other than the intended recipients." This case appears to be limited to e-mail messages that arrive at their intended destinations and are stored on a server. A different result might occur if the message is intercepted in transit, before it arrives at the intended destination. The holding of the court is broad and is likely to be challenged when a case of importance is presented and the circumstances of disclosure occur in transit before the message is received and stored. The prudent lawyer is advised not to rely on the security of passwords alone in communicating over an unsecured network with clients.

The technological problem (and thus the ethical challenge) is that such scanning receivers are in use by consumers everywhere. Likewise, the sniffer software required to intercept e-mail is commonly available. The only real difference is that the sniffer software is not (yet) considered to

[11]Edwards v. Bardwell, 632 F. Supp. 584 (M.D. La. 1986).
[12]18 U.S.C. 2520 (1996) expressly provides for a private cause of action.
[13]United States v. Maxwell, 42 M.J. 568 (US Air Force Ct. Crim. App 1995).

be a common consumer product. Using sniffer software seems confined to those who are knowledgeable in digital network communications.

These technical distinctions might well establish the reasonableness of the lawyer that creates an e-mail system with solid encryption security to ensure that client communications remain private.

There is no present consensus regarding the ethical impact of inadvertent disclosure of confidential data or information but most courts hold that inadvertent disclosure does not automatically waive the privilege.[14]

The ECPA requires that surveillance by law enforcement officials be done under a lawfully obtained and executed electronic surveillance warrant. The warrant must contain a provision that the surveillance is to be conducted in such a way as to minimize interception of privileged communications and communications not pertinent to the crime under investigation.[15] While the ECPA does not completely bar the interception of privileged e-mail, it does not alter the privileged character of the communications.

[14]*See generally*, ABA Committee on Ethics and Professional Responsibility, Formal Opinion 92-368; Bank Brussells Lambert v. Credit Lyonnais (Suisse) S.A. 160 F.R.D. 437 (DC SNY 1995).

[15]18 U.S.C 2518 (1988).