198-AUG N.J. Law. 18

New Jersey Lawyer, the Magazine
August, 1999

Feature

Jeffrey Pollock [a1]

A TANGLED WEB - THOUGHTS FOR A LAW FIRM USING THE WEB

The Internet provides lawyers with the time-saving device they desire most –the ability to rapidly and efficiently obtain information and the ability to relay that information to others. Unfortunately, the Internet is not a completely safe place for the practice of law. This article provides an overview of the concerns and solutions for law firms taking advantage of the Internet.

The Siren Call of the Internet

E-mail Provides Rapid Exchange of Data

As the "practice" of law yields (sadly) to the 1990s view that this is the "business" of law, lawyers are under tremendous pressure to develop new clients and maintain old ones. The Internet provides competing lawyers with a sharp information edge by promising rapid delivery of semiformal e-mails to clients who increasingly desire an immediate practical response more than a formal memorandum of law. Similarly, the Internet promises added freedom to the work-weary lawyer because he or she can now access e-mails from the road, from home over coffee, or during vacation. Moreover, e-mail is immediate and permits the exchange of documents, images, photographs, charts and graphs, and sound that cannot be matched by either "snail" mail or a poor quality fax.

E-mail Provides Unparalleled Information Treasures

In addition to allowing for the rapid exchange of information from virtually anywhere on the globe, the Internet is a treasure chest of information. Best of all, the fruits of your searches are often free or easily available after purchase.

Sitting in your bathrobe, you can search the entire United States Environmental Protection Agency files for guidance documents, switch in seconds to Edgar and obtain free corporate quarterly and annual reports, find a witness on Whowhere, obtain directions to your client's vacation home on MapQuest, among others, and download your stock portfolio before your coffee gets cold. Need to find out the structure of your corporate adversary or learn more about an adversary lawyer? That's all on the Web, too. Elsewhere in this issue other sources of legal research are addressed.

In short, the possibilities are limited only by your imagination and your search engine. For those of us in the business of obtaining information and using it on behalf of our clients the Internet is a dream.

*19 Concerns About Entering the World Wide Web

Fundamentally, there are two areas of concern in entering the World Wide Web (WWW) – external and internal security. The World Wide Web is the interconnected system of Internet links. Externally, there are those talented but twisted few who are going to watch where you go, what you send, what you receive, and what you do on the Web. Internally, the concern is more focused but more fatal – those dedicated stalkers that are going to seek to get inside your network, access your files, corrupt or deface your website, and perhaps intercept your emails or send false ones from your own site. There is a great deal of myth

about security on the WWW at this point in time. Unfortunately, like many of the stories we hear, there is an element of truth in these risks and many others stemming from the WWW.

Let's look at one major concern to most people, the prospect that people know where you've been and what you've downloaded on the Web.

You may be glad to know that you are not paranoid. People really are watching your every click. Those who track information on another's use of the Web are called stalkers. A stalker systematically searches for information about an individual's access to the WWW. Lest you think that stalkers are a few isolated and demented individuals, be advised that these folks are united via sites like the Stalker's Home Page. [1]

Although the likelihood of being stalked may be remote, you are undoubtedly being watched if you are on the Web. First and foremost, your own computer is betraying your privacy if you accept “cookies.” In particular, a web server can track a user's activities within that site and collect this information in a packet of information called a cookie. This cookie profiling your site use is stored on your own hard drive. This information – which the vendors claim is really for your own good – is not necessarily benign. Rather, the infection can come from the website's exchange of information about you to vendors looking for people to direct their e-mail messages to.

In addition to stalkers and non-benign cookies, there are even more intrusive search engines such as Voyeur. These search engines permit others to observe the results of your web search. [2] Even common search engines such as Altavista, Yahoo, Excite, and Lycos provide the ability to search for an individual's name, address, phone number, and neighbors. These, though, are public items of information.

Beyond the surreptitious access of a stalker or your own computer betraying you with cookies, your Internet service provider (ISP) is about to betray you as well. Virtually all netizens (Internet users for the uninitiate) access the Net through an ISP. As you are searching your way merrily along the strands of the WWW, however, your friendly ISP is collecting information regarding where you've been. The information captured is called a “click stream” and records every website you've visited. Based on an analysis of the click stream data, it is possible to identify the end user, *i.e*, you. [3]

Even Big Brother is out there looking at where you've been. The federal government is required by law to keep a hard copy of all e-mails received. [4] In your own backyard, the New Jersey Legislature has empowered the courts to order that an ISP create and release backup copies of private communications as evidence. [5]

Responding to the Problem

In addressing the lack of privacy on the WWW as an employer, first you should assume that you are being watched and let your employees know that they must assume that they are being watched, too.

Second, make sure that employees understand that they are being electronically fingerprinted every time they access a site on the Web. In reality, this may not be exactly true because it is difficult to determine accurately how many websites are collecting information on the use habits of those signing in. In addition, it is unclear whether this information is being routinely exchanged with vendors willing to pay for information regarding the identity of potential customers. But even if it turns out that some of the websites your firm is routinely using are beyond the prying eyes of stalkers, a little paranoia is good for the soul.

A third approach is to make yourself anonymous. The Anonymizer, for example, is a website that can be used to block other websites from obtaining information about you. [6] In addition to the Anonymizer, there are programs – such as Cookie Cutter and Cookie Crusher – that remove or prevent cookies from operating on your disloyal laptop. [7] Another alternative is to have a second or private web account through a second ISP, which makes it more difficult to connect your firm's ISP with a search that you conduct through a completely different Internet service provider.

In any event, the keystone of any security Internet strategy is training and vigilance. Make sure that your employees understand the risks so they act appropriately. It is also essential that your firm take action to guarantee that its training is effective and timely.

Is it Safe to Communicate Over the Net?

Although there is cause for concern about your privacy over the WWW, there is little truth to the rumor that an e-mail sent directly to a client is a risk.

***20** In reality, "it is virtually impossible to intercept an e-mail while intransit over the Internet." [8] Not only is intercepting a speeding e-mail unlikely, but there are also laws protecting the privacy of e-mail communications. [9] Notably, several early ethics opinions from other jurisdictions warned against the use of e-mail for communicating attorney-client privileged communications. It is apparent from a review of these decisions, however, that their logic is fatally flawed because they analogize e-mail communications to having the same weaknesses as do analog cellular phone calls. More recent ethics opinions recognize that e-mail is an appropriate form of protected communication between counsel and client. [10] Be aware, however, that at least one court has held that a lawyer may not be protected by the privilege that governs statements made in a judicial proceeding if those statements are made by the lawyer on the Internet in discussing the case. [11]

If you are particularly concerned about the privacy of your communications, you could install encryption software that requires the sender and receiver of the message to have a password of their own. Encryption is based on the premise that electronic data is transmitted digitally (that is, through a series of 1s and 0s). Encryption software alters the series of digits before sending the message. Upon receipt, the receiver's encryption software de-encrypts the message so that it may be read. Unfortunately, encryption software is impractical unless both the sender and recipient have the right software to transmit the message. Moreover, the United States Department of State has placed stringent controls over the export of encryption technology. [12]

In some respects, it is helpful to think of telecopies and unintended snail-mail recipients when worried about the loss of privilege or work product via e-mail. It is far more likely that you or your secretary will use the wrong fax list or mailing list, than the remote possibility that you will inadvertently type in your adversary's e-mail address. [13] In short, the possibility for sending a message to the wrong person does exist, but computers are so exacting about identification of the recipient that it remains unlikely that you will accidentally send an e-mail to an unintended party or that some "stranger" will receive your e-mail.

The Enemy Within

There are two distinct concerns from within a law firm: (a) sloppy or dangerous habits that permit an intruder to gain access to your system, and (b) intentional action by a current or former employee breaking into the network and damaging your data.

Responding to the Traitors in Our Midst

There are three major steps to take in protecting your system from internal attacks. First, train your employees on good computer protection habits. Second, configure your system's hardware and network access rights to limit individuals with access to sensitive systems. Third, be prepared for the attack of an angry current or former employee.

Training Your Employees on Good Computer Protection Habits

There are several steps employees can take to reduce the risk of permitting unintended parties access to the firm network. First, have a policy that is clear and requires employees to take appropriate action to protect the firm's computer system. For example, require the following:

1) Computers must be turned off before leaving for the day.

2) No birthdays, anniversaries or license plate numbers may be used as passwords.

3) Avoid sticky notes with passwords.

4) Avoid passwords that use names of children, spouses, or pets

5) Require periodic changing of passwords.

Configuration of Computer Systems

The primary devices for protecting against attacks from within and from without are fire walls, physical configuration (equipment placement and interconnection), and right protection (access rights which restrict the rights of each employee to specific systems). [14] A fire wall is a configuration of software and hardware that separates one system (for example, the firms website) from other systems (for example, billing, word processing, and the firm's ISP connection for e-mail and Internet research). [15] Clearly, access rights to configure and tamper with these systems must be limited to a few trusted employees.

Protection Against the Disgruntled and the Bungling

The process of protecting an entire firm network is well beyond the scope of this article. At the same time, the risk of attack through the Internet from a disgruntled current or former employee is worthy of consideration. In particular, one foreseeable scenario is that of an angry former MIS (management of information systems) employee who knows the structure of your firm's network, has numerous access rights, and probably has numerous passwords (or, worse, a listing of identifications and passwords for other employees).

Since there is always the risk of such an attack it makes sense to take several protective steps. For example, a prudent firm could periodically reconfigure its web server. [16] The system must be maintained with the most up-to-date patches and updates installed promptly by MIS personnel. In addition, the firm can use a "crack" utility to determine if there are gaps in the firm's passwords. (Such a utility runs through a list of passwords and looks for those that are likely to be readily accessible to the public.) Finally, one basic step would be to immediately eliminate access to the firm's network for any employee that has been discharged.

***21** What about hiring a hacker? Some experts recommend so-called "white hat" attacks on a firm's network in order to reveal its weaknesses. In the same vein, the MIS department should evaluate the feasibility of installing software that warns about potential unauthorized network access or irregular behaviors.

One final warning regarding system protection is to be prepared if everything fails. Considering the problems we are facing with determined hackers gaining access to sensitive Department of Energy, Department of Defense, and National Oceanic and Aeronautic Administration (NOAA) servers, it is safe to assume that many law firm servers will be even more susceptible to a determined attack. Recognizing the reality that you are vulnerable, have MIS personnel make a complete backup copy of your website and periodically back up critical data so that you can quickly restore your firm's electronic arms.

Conclusion

The good news is that e-mail appears to be a relatively safe means of communication as it stands today. There is only a limited risk that someone will install "sniffer" [17] software and breach your fire wall. If your MIS department is up-to-date and follows good management practices, the likelihood is low that your privileged communications or sensitive firm finances will ever be intercepted via the firm's e-mail system.

The bad news is that the prying eyes of the world are watching where you go and what you do on the Web. In this electronic age a prudent lawyer must assume that the risk of an intruder is real and must be addressed. Although there is relatively little to be done about what ISPs do with your Internet use data, there are a number of steps your firm can take to prevent the likelihood that an intruder will breach your firm's fire wall or that data will be otherwise surreptitiously obtained. Training and vigilance are going to be the watchwords of Internet protection as we approach the millennium. [18]

Footnotes

a1 **Jeffrey Pollock** *is a partner at Sills Cummis in Newark.*

1 The Stalker's Home page may be reached on the WWW via www.glr.com/stalk.html.

2 Wigod, Myrna, Privacy In Public and Private E-Mail and On-Line Systems, 19 Pace L. Rev. 95, 103 (Fall 1998).

3 Privacy In Public and Private E-Mail and And On-Line Systems, 19 Pace L. Rev. at 100.

4 E-mail sent or received by a government agency is subject to the Federal Records Act and must be saved in hard copy form. Armstrong v. Executive Office of the President, 877 F. Supp. 690 (D.D.C. 1995); Ballon, Ian C., The Emerging Law of the Internet, 547 Practicing Law Institute (February-March 1999)(paper presented at the 19th Annual Institute on Computer Law).

5 N.J.S.A. sec. 2A:156A (West 1998).

6 The Anonymizer is located at www.anonymizer.com. *See also*, Privacy in Public and Private E-Mail and On-Line Systems, 19 Pace L. Rev. at 141-42.

7 *Id*. At 142.

8 The Emerging Law of the Internet, p. 291.

9 Electronic Communications Privacy Act, 18 U.S.C. Secs 2510 *et seq*; *United States v. Maxwell*, 42 M.J. 568 (U.S.Air Force Crim. App. 1995), *aff'd in part*, 45 M.J. 406 (U.S.Armed Forces Ct. App. Nov. 21, 1996); and *see* The Emerging Law of the Internet, at page 290.

10 The Emerging Law of the Internet, p. 292.

11 *Seidl v. Greentree Mortgage Co.*, 67 U.S.L.W. 1335 (D. Col. 1998)

12 The Emerging Law of the Internet, at pages 285-86.

13 *See, generally*, N.J.R.E. 504.

14 Karnow, Curtis E. A., Computer Network Risks: Security Breaches and Liability Issues, 15 No. 10 Computer L. Strategist 1 (February 1999). *See also* The Emerging Law of the Internet, at page 181 and National Computer Security Association (NCSA) Firewall Policy Guide 5 (1996).

15 Web Site Security, 10 Partner's Report 10 (Institute of Management and Administration 1998). The Emerging Law of the Internet, 547 PLI at 181.

16 *Id*.

17 A sniffer is in essence a piece of software installed on your firm network and that permits information to breach the firewall. That is, it could allow your own network to transmit over the Internet information that is intended to be protected from prying eyes.

18 "But that freedom can be retained only by the eternal vigilance which has always been its price." Davis, Elmer, But We Were Born Free (1954).

198-AUG NJLAW 18

End of Document