



A Lawyer's Guide to Managing E-Lawyering Risks

from Chubb



It's Chubb. Or it's Chance.



**A LAWYER'S GUIDE
TO MANAGING
E-LAWYERING RISKS**

Prepared by

.....
*Anthony E. Davis and David J. Elkanich
Hinshaw & Culbertson LLP*

for the Chubb Group of Insurance Companies

C O N T E N T S

| | |
|---|----|
| Introduction | 3 |
| How Law Firms Are E-Lawyering | 4 |
| Internet Tools as Sources of Risk in Law Practice | 5 |
| Using Cyber Tools to Enhance Law Firm Risk Management | 12 |
| Conclusion: Seek Further Advice | 15 |
| About the Authors | 16 |

.....

INTRODUCTION: NEW REASONS TO STAY AWAKE AT NIGHT

Technology is redefining the legal profession. The ease with which clients and lawyers can access the Internet provides lawyers with an incentive to discover new techniques for delivering legal services. New and constantly improving Internet tools and software enhance the ability of lawyers and firms to manage their practices and to improve both the quality of service and the methods of delivering services to clients. The term “e-lawyering” encompasses all the ways in which the provision of legal services is based on technology. These same technological tools, however, create significant new risks for law firms. Before adopting these tools, lawyers must be aware of both the ethical and the cyber risks associated with using technology.

This booklet focuses on how lawyers and law firms can enhance their legal services to clients by adopting new technologies. It describes some of the risks involved in adopting new technologies and offers suggestions for managing those risks—sometimes through the use of other electronic tools.

HOW LAW FIRMS ARE E-LAWYERING

At one end of the e-lawyering spectrum is email, the most basic form of Internet-based communication, useful for communicating with clients and transmitting documents. At the other end, e-lawyering enables much more sophisticated service delivery. For instance, lawyers may use the Internet and its related technologies to:

- Create online chat or negotiation rooms with clients and other parties.
- Create controlled-access, case- or client-specific extranets, allowing entry only to those with permission to view some or all of a client's legal file online. Extranets permit clients and lawyers to share, in real time, document databases, docketing information, legal research and memorandums, digital copies of pleadings, and other relevant case materials.
- Create online libraries customized to particular clients or subject matter.
- Create firm blogs, or email alert systems, to keep clients apprised of recent statutory or case developments.

E-lawyering also encompasses law firms that have dispensed with the traditional firm model, opting instead for an Internet-only presence. These firms generally do not have permanent business structures among defined groups of lawyers but rather may be comprised of affiliated lawyers whose only connection is the technology linking them.

INTERNET TOOLS AS SOURCES OF RISK IN LAW PRACTICE

The Internet and its related tools can assist law firms in providing legal services to clients, but these same tools can also be sources of risk that must be monitored closely.

Risk of Unintended Client Engagements

The greatest risk to lawyers and law firms with an Internet presence is that they may not always know who their clients are. For instance, many Web sites provide prospective clients with forms enabling them to engage lawyers without any other intake processing. Other Web sites allow prospective clients to contact lawyers through email without any screening, and some lawyers spend time in chat rooms discussing legal issues. These activities pose great risks in that attorney-client relationships may be created before any evaluation for appropriateness, such as checking for conflicts of interest, has been completed.

Managing this risk: Whether an attorney-client relationship is being created turns largely on the subjective belief of the client; it is therefore important for lawyers to use appropriate screening techniques to avoid unintended attorney-client relationships. A law firm should consider the following methods of screening:

- Place a conspicuous disclaimer on the firm's Web site (or in another Internet location accessible to the public, such as a chat room) clearly stating that no attorney-client relationship exists unless and until expressly agreed to by all parties, preferably in a written engagement letter specifying (at a minimum) the identity of the client, the scope of services to be provided, and the fee arrangement.

-
- Establish appropriate screening techniques to avoid conflicts and other problematic client relationships.

A well-managed client intake process will provide that an attorney who has learned confidential information from a prospective client may be screened under American Bar Association (ABA) Model Rule 1.18, even though this would ordinarily, absent such screening, amount to a conflict imputed to the entire firm.

Risk of Disclosing Confidential Communications

The ability to communicate electronically has increased the risk of inadvertent disclosure of confidential information. Emails and other electronic communications can all too easily be directed to an unintended recipient by mistake, thereby risking a waiver of privilege. ABA Model Rule 4.4(b) addresses the obligation placed on the person who inadvertently receives a confidential document to promptly notify the sender, but significant possible malpractice exposure remains for the sender.

Accordingly, lawyers should be careful to protect confidential information when communicating electronically, whether through email, public chat rooms, or instant messaging (IM). In such situations, lawyers should use restricted means of communication, such as encryption or a client's extranet. If law firms do not take reasonable measures to ensure that their electronic communications are private and secure, there is a risk that privilege could be waived. Transmission of documents attached to electronic messages adds the risk of disclosure of *metadata*—the hidden electronic data underlying documents created in most word processing and other common software programs. For example, in a word-processing program metadata can be the redline edits associated with prior versions of the document; in a browser metadata can be the search terms inserted into a search engine. Although one opinion suggests that it is unethical for lawyers to open and view the metadata behind

documents produced by other lawyers, this is unrealistic given that clients who receive the same materials may be under no such constraints.

Managing this risk: Lawyers can avoid potential problems created by a metadata transmission by either:

- Converting Word documents to PDF or some other non-malleable format before emailing them (permitting another party to read the document but not make changes or to read a previous version); or
- Using a metadata cleaner or scrubber to erase all the metadata in a document.

Risk of Early Destruction of Electronic Documents

Practicing law electronically generates huge quantities of documents in both paper and electronic forms. Without a clear and appropriate records-management policy, early destruction of electronic documents, including email and IM records, could lead to violations of a lawyer's ethical and legal obligations. The risks posed by improper destruction of electronic documents are especially clear in the context of e-discovery. If a lawyer permits a client to destroy documents that should have been retained, or if the lawyer permits or aids a client in failing to disclose those documents that should have been discovered and produced, that lawyer may be subject to sanctions, adverse jury instructions, a mistrial or, in extreme cases, dismissal of claims—not to mention legal malpractice or spoliation claims. For example, in *Coleman v. Morgan Stanley*, Morgan Stanley stated publicly that it may sue its former counsel for the \$1.5 billion verdict it suffered because the court determined that its law firm did not respond appropriately to discovery requests for electronically stored documents.

Whenever matters involve large volumes of electronic documents, there is always a risk that lawyers requesting e-discovery will not know how to find what they are looking for. Lawyers need to be aware that electronic documents can exist in a number of different formats and locations, such as on computer networks, office and home computers, laptops, backup or disaster recovery systems, and handheld devices such as PDAs, cellular phones, and pagers. Lawyers must also consider whether documents are in a “searchable form,” whether they will be produced electronically or physically, how long it will take to produce them, and who will pay.

Managing this risk: A clear and appropriate records-management policy that governs retention and destruction of both paper and electronic documents is vital for lawyers and their clients. In every litigation that may potentially involve electronic documents, law firms must now, out of necessity, appoint someone to be responsible for overseeing their client data management to ensure that physical and electronic data are retained and are accessible as necessary to comply with discovery requirements on a timely basis.

Risk of Instant Messaging

IM, one of the newest communications technologies to enter widespread use, provides lawyers with the option of instant collaboration and real-time discussions with others who have access to the same technology. IM may be available for communications with clients and third parties. However, the use of IM raises significant risks relating to security, compatibility, and productivity. For instance, one participant may incorrectly believe his or her IM communications are not being monitored and therefore be disinclined to exercise caution. As with email, attachments may introduce viruses and other cyber problems into a network. In addition, one participant may believe an IM dialog is transitory in nature, while the other participant may be recording and keeping permanent copies.

Managing this risk: If a law firm uses IM, that usage should be closely monitored. Rather than using external providers (such as Yahoo, MSN, or AOL), a law firm should consider providing a “closed” or an internal system, allowing lawyers and staff to IM in-house. If client communication is desired, IM functionality can be placed on an access-restricted extranet to ensure security.

For these reasons, law firms should create policies governing the use of IM. Lawyers and staff should be made aware that:

- Personal IM use must be consistent with the restrictions spelled out in the firm’s email and Internet policies, and
- They should have no reasonable expectation of privacy with IM (any more than they do with email or any other Internet usage).

Because all IM communications are inherently electronic, law firms need to consider which IM communications need to be collected and stored and how to do so. Law firms should include IM in their document retention and destruction, general technology, and e-discovery policies.

Risk Arising from the Unauthorized Practice of Law

Because Web sites are, by definition, accessible from any computer providing Internet access, lawyers need to be aware of the dangers of practicing—or in some circumstances even communicating—over the Internet in jurisdictions where a lawyer is not licensed and/or a law firm has no permissible presence due to the risks associated with unauthorized practice of law. Although a lawyer cannot control who has access to a firm’s Web site, accepting clients over the Internet makes the lawyer vulnerable to accusations that the lawyer is practicing law in jurisdictions where he or she is not authorized to do so. Email messages, IM, and chat rooms raise questions about whether and when a lawyer is giving advice in another jurisdiction,

and marketing legal services to prospective clients in other jurisdictions certainly heightens this risk. Even participation by lawyers in blogs or virtual libraries can raise questions as to whether these activities can be construed as giving legal advice.

Using the Internet and its related technologies may also subject a lawyer to the jurisdiction of a foreign court, even if the lawyer never leaves his or her home state. On the one hand, a passive law firm Web site that does not allow client interaction would likely not subject the law firm to jurisdiction in a foreign court. On the other hand, when the law firm actively engages in e-lawyering, the risks increase. In one recent case, the court held that a New York law firm was subject to suit in Kansas when it represented clients based in Kansas against a Delaware corporation; the email and telephone communications with clients were sufficient to establish minimum contacts even though the matter was managed entirely from the firm's New York office and no lawyer from the firm ever set foot in Kansas. Other consequences of law practice in jurisdictions in which lawyers or firms are not authorized to practice may include fee forfeiture, professional discipline (in the host and/or home state), or even criminal prosecution.

Managing this risk: Some lawyers attempt to resolve these risks by including disclaimers on their Web sites. Others require clients to provide information about client identity and location before agreeing to accept engagements. Lawyers may wish to consider what client and matter intake screening mechanisms are appropriate in order to avoid allegations of unauthorized practice of law.

Risk of Security Breach

Any use of the Internet and its related technologies opens a lawyer or law firm up to electronic risks such as viruses and security holes, unauthorized users, unauthorized software, and spyware. Such

breaches could lead to the dissemination of confidential information, harming and embarrassing clients, and even to the potentially disastrous loss of work product, client information, and electronic documents. Notably, recent decisions have held that even the accidental and unintended destruction of electronic documents—e.g., by a computer virus—does not relieve a lawyer of the duty to maintain records.

Managing this risk: Lawyers and law firms need to take reasonable measures to ensure that client information and work product are protected in a secure environment. All firms should update and review their networks; back up resources on a regular basis; install the latest firewall and virus protection software and the latest software updates; be on the lookout for viruses, spyware, and adware; and promptly identify and resolve any security breaches that do occur.

USING CYBER TOOLS TO ENHANCE LAW FIRM RISK MANAGEMENT

It is clear that using cyber tools can bring accompanying risks. Yet such tools can also enhance risk management efforts in numerous ways.

Assisting Client Intake Management

A variety of software packages exist that can enormously improve a law firm's ability to manage client intake in a uniform and an effective manner, in single and multiple locations. Technology can be used to flag conflicts of interest in "real time." Such technologies enable firms to effectively, consistently, and efficiently manage client intake. But in order for this to work, a number of factors need to be present:

- Everyone in the firm must use the system, use it in the same way, and use it promptly.
- The information included must be comprehensive, including all parties to the matter.
- The information must be regularly updated and maintained.
- Conflicts of interest and the client intake system should be centrally managed.

Improving Law Firm Management

As other businesses do, law firms can use the Internet and its related technologies not only to enhance service delivery to clients but also to improve the management of their financial and business affairs. For example:

- Time-recording and billing software has led to advances in fee and billing management, offering management tools to monitor

firm-wide client billing and receipts and to ensure that lawyers regularly input their timekeeping and billing activities.

- Firm-wide docket and calendaring systems allow management to centralize calendaring, ensuring a uniform process for scheduling court dates, due dates, and ticklers. This eliminates the inherent problems of having many individual calendaring systems and facilitates firm or practice group oversight to ensure deadlines are met. If a client extranet includes the case calendar, the client can save the time of a call to the firm altogether by accessing the information online.

Centralizing Case Document and Information Management

Software now enables a law firm to manage an entire case file online on the firm's intranet or extranet. All documents, records, and work product—including email—can be stored in one electronic file so that all who need access can have it. Such centralized control permits the firm to regulate access to this material, allowing clients and lawyers to review this material remotely while screening out those who are not entitled to access.

At least one state bar has issued an ethics opinion stating that a law firm may use wholly electronic case files, without paper backups, as long as a client's interests are not prejudiced by this system. A benefit of using electronic case and matter files is that everything in the files can be accessed anytime, from anywhere, from any computer with Internet access. However, there are, of course, instances where original documents, such as wills and marriage certificates, must continue to be stored.

Using an Intranet/Extranet Project Manager

A law firm may find it valuable to appoint a project manager to develop and manage intranets and extranets—valuable resources that

can provide a wealth of information to firm lawyers and clients. For example, properly developed intranets and extranets make it possible for firms with offices in multiple locations to enhance their human resources and practice group management, case management, and research. A project manager can be integral to a virtual library on the Internet because he or she can, *inter alia*, update the library, date all versions of materials added to the library, and create and place disclaimers. Moreover, a project manager can be the first to identify and stop problems with technology breaches, such as viruses and spyware.

Planning for Disaster

A law firm can use the Internet and related technologies in developing disaster recovery plans. A firm needs to have data backup systems and ensure that data are saved on network servers rather than on personal computers. Backup systems should also be regularly tested.

CONCLUSION: SEEK FURTHER ADVICE

This booklet raises a number of important issues surrounding e-lawyering risks and offers practical suggestions for managing those risks. It was written to help lawyers who use Internet-based tools in their law practices. However, this booklet is not intended to be a substitute for legal advice that can only be obtained from a qualified lawyer with appropriate expertise who is familiar with each client's circumstances. The authors urge readers who intend to practice law using new technologies to seek qualified professional advice.

ABOUT THE AUTHORS

Anthony E. Davis

Anthony Davis, a partner in the Hinshaw & Culbertson LLP law firm and a member of the firm's *Lawyers for the Profession*[®] practice group, advises attorneys and law firms on legal professional and ethics issues; law firm creation, merger, and dissolution; and issues relating to risk management and loss control. He is the author of *Risk Management Survival Tools for Law Firms* and *The Essential Formbook: Comprehensive Practice Management Tools for Lawyers*, published by the ABA, and he writes a bimonthly column on professional responsibility in the *New York Law Journal*. He received his law degree from Cambridge University and an LL.M. from New York University School of Law.

David J. Elkanich

David Elkanich, an associate in the *Lawyers for the Profession*[®] practice group at Hinshaw & Culbertson LLP, regularly speaks and writes about professional responsibility and risk management. He is currently co-editing the *Oregon Ethics Opinions* to reflect the change from the *Code of Professional Responsibility to the Rules of Professional Conduct*. He is co-author of the quarterly publication *The MPC Risk Manager* and of a regular column on the Oregon State Bar Litigation Web site titled "American Legal Ethics." He received his law degree from the University of Oregon School of Law.

Hinshaw & Culbertson LLP

The *Lawyers for the Profession*[®] practice group of the Chicago-based law firm Hinshaw & Culbertson LLP provides a wide range of professional responsibility and risk management services to law firms and lawyers from 28 offices around the United States.



Chubb Group of Insurance Companies

Warren, NJ 07059

www.chubb.com

This document is advisory in nature. It is offered as a resource to be used together with your professional insurance and legal advisors in developing a loss control program. This guide is necessarily general in content and intended to serve as an overview of the risks and legal exposures discussed herein. It should not be relied upon as legal advice or a definitive statement of law in any jurisdiction. For such advice, an applicant, insured, or other reader should consult their own legal counsel. No liability is assumed by reason of the information this document contains.

For promotional purposes, Chubb refers to member insurers of the Chubb Group of Insurance Companies underwriting coverage.

Form 14-01-0948 (Ed. 10/06)