THURSDAY, MAY 4 **3:30 p.m. – 5:15 p.m.**

PRACTICE MANAGEMENT GROUP: DANCING WITH THE DEVIL - HOW TO PROTECT YOURSELF AND YOUR CLIENT'S CONFIDENCES IN AN INSECURE WORLD

GROUP AND PROGRAM CHAIR:

Michael Goler

Goodman Weiss Miller LLP, Cleveland, OH

SPEAKER:

William Freivogel

AON Risk Services, Professional Services Group, Chicago, IL

Dancing with the Devil: How to Protect Yourself and Your Client's Confidences in an Insecure World

Thursday, May 4, 2006, 3:30-5:15 p.m.
San Diego, California

I. INTRODUCTION

II. E-MAIL (OR, THE KEYBOARD IS YOUR ENEMY)

A. "Aren't these E-mails Privileged or Work Product?"
B. "Our Firm Deletes All E-mails after Six Months."

III. VOICEMAIL

IV. ENCRYPTING E-MAIL

V. METADATA

VI. BACKING-UP DATA

VII. LAW FIRM WEB SITES

VIII. INSTANT MESSAGING

IX. QUICK TAKES

Delete
Wireless communication
Cellular and portable telephones
E-mail and the reply to all function
Facsimiles: speed dial and broadcasts
E-mail and facsimile privilege/work product/confidentiality disclaimers
Speakerphones: buttons
Listservs and blogs
Phishing
Spyware
Viruses
Trojans

TECHNOLOGY AND THE LAWYER'S DUTY OF CONFIDENTIALITY

By William Freivogel
Aon Risk Services, Professional Services Group

I. INTRODUCTION

This paper focuses on the information technology that sophisticated law firms use, and on the ways this technology can be misused.

It is assumed that readers are with law firms or other organizations that have reasonably sophisticated information technology staffs. This paper will, therefore, avoid discussing here such basic subjects as network design, hardware and software selection, lawyer and staff training, security implementation (firewalls, etc.), viruses and spy-ware, maintenance of intranets and extranets, and password protocols. This paper will discuss those subjects that, for one reason or another, require the involvement of lawyers and top law firm administrators.

II. E-MAIL (OR, THE KEYBOARD IS YOUR ENEMY)

Lawyers must understand that they cannot be sure that their E-mails will not be turned over to prosecutors, regulators, plaintiffs in cases where the client's conduct is at issue, and plaintiffs in suits against the firm. A lawyer beginning to compose an E-mail message must assume that she will be asked on the witness stand to read and explain the message to a jury. Where possible, that lawyer should consider foregoing E-mail and having a private conversation with the intended recipient. This is particularly true where the subject or theme of the message is the conduct or competence of a lawyer in the firm, or that of the client. It is also true when a lawyer believes he has made a mistake. When the conduct of a lawyer in the firm is at issue, convey related information orally to the person in the firm designated to handle such matters (for our purposes in this article, the "General Counsel"). If the General Counsel needs something written, it can be prepared under the General Counsel's supervision.

A. "Aren't These E-mails Privileged or Work Product?"

Good luck. For those who do not follow claims against law firms, the biggest problem for good law firms is client fraud in the business practice. At this writing there have been thirty-six settlements by law firms exceeding $20 million, the largest being $108 million. Thirty of those, including the largest, involved fraud by a client and subsequent claims by third parties against the client's law firm. The attorney-client privilege evaporates in these cases, and the law firms must turn over their E-mails to prosecutors, regulators, and class action plaintiffs' lawyers. This includes E-mails to and from clients, and E-mails between and among lawyers in the law firm. The ways that the

privilege can be lost are myriad. A court can make a "crime/fraud" finding.[1] The client can waive the privilege as a public relations gesture.[2] A bankruptcy trustee or examiner can waive the privilege for an insolvent client.[3] Waiver can be part of a plea agreement.[4] Sharing documents with regulators (even with a confidentiality agreement) may cause a waiver in class actions or derivative actions.[5]

As to communications within a law firm about potential claims against the firm, courts do recognize an intra-firm attorney-client privilege. Problems arise, however, where the claimant is a current client. In such cases, courts have held that the firm's conflict of interest abrogates its attorney-client privilege.[6]

B. "Our Firm Deletes All E-Mails After Six Months"

Again, good luck. Your clients don't. Third-party recipients don't. If you print your important E-mails, the hard copy is still in the paper file. If your software permits you to put E-mails in special folders (What system does not?), they are still there. It is doubtful that any law firm anywhere purports to delete E-mails after a given period that also deletes messages kept in such folders. In short, E-mails are everywhere and are forever.

III. VOICEMAIL

E-mails that are negative about lawyers or clients are dangerous; such sentiments should be conveyed orally. This does not mean that lawyers should do so by leaving a message on someone's voice mail. Firms and companies are increasingly saving or backing up voicemails. That means when the attorney-client privilege is lost, or when the firm is sued, recorded voicemail becomes available to prosecutors, regulators, and plaintiffs' lawyers. Thus, the most that lawyers should say on voicemail when they have

---

[1] *See* RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS § 81 (2000) [hereinafter RESTATEMENT] (discussing privilege); *id*. § 93 (discussing work product).

[2] Several law firms representing Enron saw their communications with and about Enron made public. *See* Testimony of Stephen Hall before the Senate Committee on Commerce, Science, and Transportation, May 15, 2002.

[3] *See, e.g.,* FDIC v. Cherry, Bekaert & Holland, 131 F.R.D. 202, 205 (M.D. Fla. 1990); Odmark v. Westside Bancorp., 636 F. Supp. 552, 554-56 (W.D. Wash. 1986). As to the Examiner in the Enron bankruptcy waiving Enron's privilege, see In re Enron Corp., Order Pursuant to 11 U.S.C. §§ 1104(c) and 1106(b) Directing Appointment of Enron Corp. Examiner, No. 01-16034 (AJG) (S.D.N.Y. Apr. 8, 2002).

[4] For a good overview of how the Department of Justice uses this technique, see John Gibeaut, *Junior G-Men*, A.B.A. J., June 2003, at 46.

[5] *See, e.g., In re* Columbia/HCA Healthcare Corp. Billing Practices Litig., 293 F.3d 289, 302-04 (6th Cir. 2002).

[6] For an article critical of this result, see Douglas R. Richmond, *Law Firm Internal Investigations: Principles and Perils,* 54 SYRACUSE L. REV. 69 (2004).

something negative to convey is "please give me a call or come see me." If the call is returned, presumably the conversation can occur with relative safety.

IV. ENCRYPTING E-MAIL

Encryption software makes E-mail messages unreadable, unless the recipient has a "code" or "key" to make the message readable. Occasionally, well-meaning experts in law firm risk management advocate that law firms encrypt their outgoing E-mails and require their clients to do the same.[7] That position has two problems. First, encryption software is cumbersome. Second, most clients—even large and sophisticated clients—do not use encryption, and do not want their lawyers to use it. Therefore, life for lawyers, their law firms, and their clients will be easier without encryption. The vast majority of state ethics bodies and the ABA's Standing Committee on Ethics and Professional responsibility agree that the ethics rules do not require encryption.[8] Using unencrypted E-mail does not waive the attorney-client privilege.[9] Last, in all the author's years of advising law firms on loss prevention and studying claims against law firms, he is not aware of a single instance in which a lawyer or law firm paid civil damages resulting from the interception of an unencrypted E-mail.

V. METADATA

Documents created with word processing software contain "metadata."[10] Metadata is information embedded in a document's electronic file that is automatically created by the software the author is using without the author's intent or knowledge. Metadata may include the author's name, the names of prior authors, the identity of the server or hard drive where the document is saved, when the document was created, file properties and summary information, document revisions and versions, template information, the names of people to whom the document has been sent, comments, the time spent editing the document, custom document properties, and more. "Metadata can be as revealing as a postmark on a letter, fingerprints on the envelope, and DNA from

---

[7] A report of a law firm "audit" recently conducted by a law firm risk management consultant, who, in the course of advising the firm to encrypt its E-mail, asserted that all good firms encrypt E-mail. That statement is, of course, not true.

[8] *See, e.g.,* ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 99-413 (1999); Del. State Bar Ass'n, Comm. on Prof'l Ethics, Op. 2001-2 (2001). For an excellent discussion of unencrypted E-mail, see David Hricik, *Lawyers Worry Too Much About Transmitting Client Confidences by Internet E-mail,* 11 GEO. J. LEGAL ETHICS 459 (1998). For a compilation of state authorities, go to David Hricik's Web site at http://www.hricik.com/email.html (last visited Oct. 11, 2005).

[9] *In re* Asia Global Crossing, Ltd., 322 B.R. 247, 256 (Bankr. S.D.N.Y. 2005).

[10] David Hricik & Robert R. Jueneman, *The Transmission and Receipt of Invisible Confidential Information,* PROF. LAW., Spring 2004, at 18, 18; Jason Krause, *Hidden Agendas,* A.B.A. J., July 2004, at 26, 26; Donna Payne & Bruce Lewis, *What You Can't See, Can Hurt You,* LEGAL TIMES, Sept. 27, 2004, at 16, 16; Thomas E. Spahn, *Litigation Ethics in the Modern Age,* BRIEF, Winter 2004, at 12, 16.

saliva on the seal."[11] Furthermore, because lawyers often reuse documents and templates, the amount of metadata that a document contains is often impossible to judge.

Many lawyers know that documents transmitted electronically contain metadata. One lawyer has even boasted publicly that "'[t]he first thing I do when I get something is look for [metadata] like the author's name, revisions, and history.'"[12] The problem, quite obviously, is the associated transmission of confidential information.[13]

Given lawyers' ethical obligation to maintain clients' confidences, they should exercise reasonable care to strip metadata from documents exchanged with adversaries, electronically filed with courts, or disclosed to the public. Various types of scrubbing software are available. Alternatively, lawyers might transmit documents in electronic formats that do not allow metadata to be revealed. For example, documents in "pdf" format contain much less of such data. If you have reservations about particular documents, and can do so, one solution is to send paper copies.

The practical problems posed by metadata transmission are several. Suppose that you send a client a bill as an E-mail attachment, or put the bill on a shared drive or intranet accessible by the client. Suppose further that the client uncovers the metadata in the bill, and it reveals that you changed the amount charged for "secretarial overtime," which the client said it would not pay for, to "photocopying expense," which the client agreed to pay for.[14] Alternatively, suppose that you are negotiating a settlement, and you send a proposed settlement agreement to the lawyer on the other side. The parties have not yet agreed on the amount. The initial draft contains a settlement amount of $15 million. Your opponent opens the hidden data, which suggests that your client was willing to pay $30 million. No firm wants to find itself in one of these situations.

Since the threat to client confidentiality and attorney work product posed by metadata is now known, it is appropriate to focus on the lawyers who receive electronic documents loaded with invisible information. Do they have any ethical obligations with respect to the metadata hidden in the documents sent to them? On the one hand, it might be reasonably argued that lawyers' duty to competently represent their clients obligates them to uncover the metadata in the documents they receive and, if possible, use any information revealed to their clients' advantage. On the other hand, it can just as easily be argued that electronically ransacking a document to uncover metadata is dishonest—it

---

[11] Krause, *supra* note 10, at 26.

[12] *Id.* (quoting lawyer).

[13] *See id.* (describing confidential information learned from an examination of metadata found in a document from a major intellectual property lawsuit).

[14] This is not a hypothetical. A partner in a very fine law firm did this to several large corporate clients, and when caught, was disciplined. The law firm had to reimburse the clients for the over-billings. The aggravation and embarrassment were substantial.

is no different than rummaging through another lawyer's briefcase when he leaves the room, or eavesdropping on another lawyer's private conversation with her client.

The New York State Bar Association's Committee on Professional Ethics attempted to resolve this debate in a 2001 ethics opinion.[15] The Committee saw no difference between a lawyer's surreptitious examination of metadata and "less technologically sophisticated means of invading the attorney-client relationship" that have been "rejected as inconsistent with the ethical norms of the profession."[16] The Committee concluded that a lawyer's surreptitious use of technology to obtain another party's potentially confidential information would violate New York's ethics rules prohibiting conduct involving dishonesty, deceit, fraud or misrepresentation, and conduct prejudicial to the administration of justice.[17]

VI. BACKING-UP DATA

All law firms back-up data, but the ways they do it differ dramatically. On one extreme, a firm might back up information for just one week. On the other extreme, a firm might conclude that the best system is to maintain a bank of inexpensive servers and keep everything forever. There are law firms at both extremes and many in between. In any event, it is the rare law firm that can know with absolute confidence what data exist and what do not. Here is an experiment that law firm risk managers might conduct: go to the appropriate person and request to see backed-up data within certain parameters and from a certain time. There have been instances where a court ordered an entity to produce backed-up data, and the entity only then learned that the system was not working and, perhaps, had never worked. No one had bothered to check.

VII. LAW FIRM WEB SITES

Various states have advertising regulations dealing with law firm web sites. Those regulations do not deal with confidentiality, so this paper will not discuss them. One troublesome circumstance is the law firm's receipt of prospective client messages resulting from an invitation on the firm's web site.[18] The message may contain all kinds of confidential information about the sender. The firm promptly discovers that it either is on the other side of the matter or surely will be. But, the firm has a duty of confidentiality to prospective clients, even though they do not become actual clients.[19] Thus, the firm may be disqualified from handling the matter.

---

[15] N.Y. State Bar Ass'n Comm'n on Prof'l Ethics, Op. No. 749, 2001 WL 1890308 (Dec. 14, 2001).

[16] *Id.* at *2.

[17] *Id.*

[18] For a detailed discussion of this subject, see David Hricik, *To Whom it May Concern: Using Disclaimers to Avoid Disqualification by Receipt of Unsolicited E-mail from Prospective Clients*, PROF. LAW., No. 16-3, at 1 (2005).

There are two possible solutions to this, neither perfect. First, put on the site a statement admonishing the reader not to send confidential information to the firm until the reader has a signed engagement letter, and explaining that the law firm may be, or may in the future be, on the other side. The placement of the admonition may be important. There are sites that cannot be accessed until the reader clicks on a button directly under such an admonition that says "I Agree." Other sites merely provide a link to a disclaimer—usually at the very end of the message. In some cases the link appears in very small type. The first two options are more desirable than the third, and disclaimers need to be obvious in any event.

Another safety valve is to limit access to such messages to just one designated lawyer or staff person, who will run a conflicts check. Provide in writing in a firm policy or directive that if a conflict is detected, the designated person will not communicate the contents of such messages to anyone else in the firm, will reply to the sender that the firm cannot be involved, and will then delete the incoming message. There appears to be no rule, ethics opinion, or case that approved of such a screen as a way to avoid disqualification, but the firm's chances of avoiding disqualification are probably better with such a procedure in place.

VIII. INSTANT MESSAGING

Use of this technology is growing rapidly, and no one has a complete handle on the risks to law firms using it. Instant messaging can be a two-edged sword. Given the configuration, the messages may not be saved or archived. That is good to the extent it prevents discovery of "smoking guns." It is bad, however, if the lawyer needs to document the advice the lawyer gave during an instant messaging exchange. There are ways to ensure that messages are saved—another two-edged sword, of course. If a law firm is going to provide or permit instant messaging, it must know exactly where the system stands with respect to archiving and then train lawyers and staff on the same issues raised by E-mails. Here again, the keyboard can be your enemy.

IX. QUICK TAKES

Following are brief reminders of the relationship of confidentiality to information technology, which on one level should be obvious, but which still bear repeating.

Delete. When you delete parts of a document, you are not removing the data from the hard-drive. Unless the drive is full, the data remains. You just do not see it anymore. This data is relatively easy to find and recover.

Wireless communication. The ability to communicate wirelessly with a computer takes many forms. All such communications are relatively insecure. Avoid transmitting anything sensitive to, or about, a client when in wireless mode.

---

[19] RESTATEMENT, *supra* note 1, at § 15.

Cellular and portable telephones. Cellular phones are relatively secure. In contrast, portable telephone (the kind used around the house) conversations can be intercepted accidentally with something as low tech as a baby monitor.

Flash drives. Flash drives are those little sticks that enable a user to move data from one computer to another. It would be bad to leave one in a coffee shop or airport boarding lounge if it contained sensitive client information.

E-mail and the reply to all function. The reader as undoubtedly read of incidents in which lawyers who use the "reply to all" function common to all E-mail systems embarrass themselves. The latest example comes from Kansas City, Missouri. The following names are fictitious. Andrews E-mailed Baker, an associate at Charles & Davis, to ask whether Baker's client would voluntarily dismiss a claim against Andrews's client, or whether he should file a motion to dismiss. Ever the good subordinate, Baker forwarded Andrews's inquiry to Charles, the partner for whom he worked. Charles hit the "reply to all' button on his E-mail, thus replying to Andrews instead of just to Baker. His message, cleaned up a bit, was this: "Make the [knuckle]head work for it. It might be different if he wasn't such [a body part]." As is typical in dustups like this, Andrews forwarded Charles's profane E-mail to lawyers throughout Kansas City, some of who disseminated the message further. Beyond that sort of embarrassment, it is easy in this case to envision the E-mail attached as an exhibit to a motion for sanctions.

Facsimiles: speed dial and broadcasts. The stakes are high when you or a staff person hits the wrong speed dial number, particularly when speed dial is combined to a multi-party, or "broadcast," feature.

E-mail and facsimile privilege/work product/confidentiality disclaimers. They are overused and may not be effective. The author knows of no cases one way or the other. The wording selected seems to be inconsequential. Probably those that appear at the beginning of the message have a better chance of succeeding than those appearing at the end. Disclaimers are no substitute for using great care in composing and addressing the message or document. *Caution, though*: firms that do federal tax work should continue including the statement required by IRS Circular 230 unless and until developments suggest otherwise.

Speakerphones: buttons. When hanging up, pick up the receiver, and put it down. Do not trust the "off" button to work, or trust yourself to hit the correct button.

Listservs and blogs. Remind firm lawyers and staff that they are to post nothing about a client matter—including even the identity of the client—on a listserv, blog, or electronic bulletin board.
