

Technology and Confidentiality

From the Committee on Professional Responsibility, William Freivogel, Chair

The January 2009 issue of “Ethics Corner” discussed generally the duty of confidentiality under legal ethics rules. That article briefly mentioned several technology issues. The purpose of this article is to expand on those issues and add several.

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. 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 is 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. *See* American Bar Association, Standing Committee on Ethics and Professional Responsibility, Formal Op. 99-413 (1999), and the state and local opinions cited therein.

Metadata. In the October 2007 issue of eSource we discussed in some detail the dangers posed by metadata in documents prepared by lawyers and transmitted to third parties. We will not repeat that material here. One of the things we noted was that various state ethics committees have taken different positions on whether it is unethical for lawyers to try to recover metadata from documents received from adversaries. More recent opinions reveal that those differences persist. *See, e.g.*, State Bar of Arizona Ethics Committee Op. 07-03 (2007) (unethical); Professional Ethics Commission of the Board of Overseers of the Maine Bar Op. 196 (2008) (unethical); Pennsylvania Bar Association Committee on Legal Ethics and Professional Responsibility Op. 2007-500 (2008) (it depends); and Colorado Bar Association Ethics Committee Op. 119 (2008) (it depends). The important message here is that it could be dangerous for a lawyer to seek to extract metadata from adversaries’ documents, and any lawyer thinking about doing so had better double check his or her state’s position.

Law Firm Web Sites. Law firms must pay close attention to what client information appears on their Web sites. For example, the propriety of identifying clients on law firm Web sites is highly questionable absent consent from the clients. *See* Paul R. Tremblay, *Migrating Lawyers and the Ethics of Conflict Checking*, 19 Geo. J. Legal Ethics 489 (Spring 2006). Professor Tremblay makes a compelling case that the identity of a client is protected information under ABA Model Rule 1.6, the core confidentiality rule.

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.

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. One problem with cellular telephones is not the technology; it is the lawyers using them. Who has not heard confidential information being discussed on cellular phones in restaurants, in airplanes, in elevators, etc? Quite recently a department head of a prestigious law firm was overheard on a train loudly discussing by name all the lawyers in his firm that were about to be laid off, Amanda Royal, *The Recorder*, Feb. 20, 2009.

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 client information.

E-mail and the "Reply to All" Function. The reader has 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 delicate 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 with a multi-party, or "broadcast," feature.

E-mail and Facsimile Privilege/Work Product/Confidentiality Disclaimers. They are overused and may not be effective. 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. Here are two opinions dealing with lawyers who misused speakerphones and revealed client confidences to adversaries: *Jasmine Networks, Inc. v. Marvell Semiconductor, Inc.*, 117

Cal. App. 4th 794 (Cal. App. 2004); and *Howell v. Joffe*, 483 F. Supp. 2d 659 (N.D. Ill. 2007).

Listservs and Blogs. Lawyers are to post nothing about a client matter—including even the identity of the client—on a listserv, blog, or electronic bulletin board. American Bar Association, Standing Committee on Ethics and Professional Responsibility, Formal Op. 98-411 (1998) is apt. The opinion contains a discussion of what a lawyer (“Lawyer A”) may reveal to another lawyer (in a different firm) (“Lawyer B”) when the Lawyer A is seeking the Lawyer B’s informal advice on a matter Lawyer A is handling. The opinion cautions that Lawyer A should not reveal the identity of Lawyer A’s client. It further cautions that if Lawyer A “disguises” (our word) the matter to avoid revealing such information, the disguise had better be a good one, so Lawyer B cannot figure out who is involved. Many lawyer-oriented listservs and blogs are for just such consultations, and the reasoning of Op. 98-411 applies.

Disposing of Computer Equipment. Technology staffs of well-run law firms know how to clean the hard drives of equipment that is being scrapped or sold. Otherwise, the dangers of client information seeing the light of day in these situations can be great.

“Mystery” E-mails. Most lawyers now know this, but it bears repeating: do not open E-mail attachments unless you are positive that the E-mail is legitimate. If you receive an E-mail that you were not expecting, do not open any attachments unless you have confirmed the message is legitimate. This is true even where you recognize the sender, but were not expecting the message. Only when you receive a message you were expecting is it probably safe to go ahead and open the attachment. Failure to observe these fairly simple directions could expose client data on your computer as well as client data on your firm’s entire network.
