# Ethics Watch

## *Technology and Confidentiality, Part One*

*By Nathan M. Crystal*

If you ask lawyers to list their most important ethical obligations, confidentiality will certainly be included by almost all of them. Complying with this fundamental ethical duty, however, has become increasingly difficult and risky with the widespread use of modern technology in the practice of law.

The basic obligation of lawyers with regard to confidential client information is clear: lawyers must take reasonable steps to protect the confidentiality of such information. South Carolina Rule of Professional Conduct (SCRPC) 1.6, comment 18 states: "When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients." However, it is often difficult to determine what is reasonable and to implement reasonable precautions when using modern technology. In the next two columns, I plan to examine these questions. In these short articles I cannot hope to give these issues a complete treatment, but I will attempt to highlight major problem areas, identify some important resource material, and offer to lawyers and law firms some modest practical suggestions for dealing with these difficult issues. In this first column I will address (1) public use of technology, (2) metadata in document transmission, (3) loss of devices, and (4) disposal of devices. The second column will consider (5) outsourcing and "the cloud," (6) use of social networking sites, and (7) dealing with confidentiality breaches. In the second column I will also suggest one way of addressing these issues—development of law firm policies on these issues and inclusion in the firm's engagement agreements of a provision summarizing the firm's policies with regard to the use of technology, seeking client consent to those policies, and inviting clients to inform their lawyers if they wish the firm to use different approaches if feasible. With regard to many of these issues, lawyers need to employ competent IT personnel to give advice with regard to technical issues and implementation of appropriate policies. In addition, firms can find on the Internet policies used by business organizations that deal with sensitive data. This public information can be very helpful to law firms as a checklist in developing and implementing their policies. See, e.g. Sans Institute, *Information Security Policy Templates* (available on the Internet). For a bibliography on confidentiality and technology, see ABA Comm. on Ethics 20/20 Working Group on the Implications of New Technologies, *Client Confidentiality and Lawyers' Use of Technology* (September 10, 2010).

### Public use of technology

Do you know or have you heard a lawyer discussing a client matter in public on a cell phone? If so, is this lawyer using reasonable precautions to protect the confidentiality of client information? With regard to cell phones, it should be pretty obvious that discussing sensitive client matters in public where they could be overheard by anyone is not a sufficient protection of confidentiality. The solution is clear—don't do it. If you need to make a call about a client matter, don't make it until you can do it in a reasonably confidential place. If you receive a call from a client in a place that is not confidential, don't take it. Clients will understand and appreciate when you say "Let me call you back in about 15 minutes when I can speak with you confidentially." Of course, there are some calls related to client matters that can probably safely be taken even in a public setting, for example a call from the lawyer's secretary confirming a meeting time. If you are talking about something routine that does not reasonably appear to be confidential and you don't need to reveal any identifying client information, then the call should be ethically permissible. But caution is the best approach; when in doubt "don't make it or take it" until you can do so confidentially.

Do you know or have you heard of lawyers using public Internet sites to research and communicate about client matters? Use of computers for handling client matters on public networks, such as ones at Starbucks, at airports, or in other hotspots, runs the risk that information may be hacked. On the other hand, lawyers are often traveling away from their offices where secure networks are not available. Undue restrictions on the use of such networks could significantly hamper the work of many lawyers. In Formal Opinion 2010-179, the California Ethics Committee warned lawyers about the use of such networks:

> With regard to the use of a public wireless connection, the Committee believes that, due to the lack of security features provided in most public wireless access locations, Attorney risks violating his duties of confidentiality and competence in using the wireless connection at the coffee shop to work on Client's matter unless he takes appropriate precautions, such as using a combination of file encryption, encryption of wireless transmissions and a personal firewall. Depending on the sensitivity of the matter, Attorney may need to avoid using the public wire-

less connection entirely or notify Client of possible risks attendant to his use of the public wireless connection, including potential disclosure of confidential information and possible waiver of attorney-client privilege or work product protections, and seek her informed consent to do so.

The opinion might not be correct in light of ABA Formal Opinion 99-413, in which the ABA Ethics Committee advised that lawyers could use e-mail without encryption because there was a reasonable expectation of privacy with regard to e-mail and because interception of e-mail was criminal. While the expectation of privacy with regard to the use of public networks is undoubtedly less than when lawyers use their own systems, such an expectation still exists to a large degree. Indeed, how much of an expectation of privacy do lawyers realistically have when they use their own e-mail systems? E-mails they send will be on their servers, in the recipient's server, in the provider's server, and in the sender's and recipient's smart phones or tablets. Moreover, interception of communications on public networks would also be criminal. The comments to Rule 1.6 support this view that special precautions are generally not necessary with regard to the use of a method of communication:

> This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement.

In my view lawyers should generally be allowed to use public networks without special security measures unless the matter is particularly sensitive (a public offering of securities or a high profile litigation case, for example) or the client has directed otherwise. The issue of use of public networks can appropriately be included in the section of the firm's engagement agreement that deals with the use of technology. I will discuss such a provision in the second column on this topic. Of course, lawyers or their firms can adopt greater precautions if they feel that these are necessary in light of the nature of the case or the industry in which the client operates. A lawyer could follow the recommendations of the California opinion, but a lawyer might take steps that were not as substantial. For example, the lawyer could do research of a client matter using a public network, but might then sign off when writing an opinion letter to the client.

This view finds support in cases like *Stengart v. Loving Care Agency, Inc.*, 990 A.2d 650 (N.J. 2010), which held that the attorney-client privilege applies to e-mails sent by a client who was an employee to her attorney composed on company-owned computers even though the company had a policy allowing review of such e-mails, albeit an ambiguous one. It seems to me that the expectation of privacy in public networks is greater than the expectation of privacy in e-mails on employer-owned computers when the employee has received notice that the employer can access and review such e-mails. See also *Client Confidentiality and Technology*, *supra* at 2.

### Metadata in document transmissions

Metadata refers to information embedded in electronic documents, such as the date of creation, changes made, author and date of changes, date of last saving, and comments. In ABA Formal Opinion 06-422, the ABA committee advised that a lawyer who received a document from opposing counsel in connection with a matter could ethically access and review the metadata contained in the document. The committee concluded that no rule specifically pro-

hibited a lawyer from examining the metadata. It decided that Rule 4.4(b) dealing with inadvertently produced material did not apply because a document sent to opposing counsel was not done inadvertently.

Ethics committees in some states have taken a different view from the ABA committee on review of metadata, relying on the principle that examination of metadata by opposing counsel is a form of dishonesty. See the opinions in New York and Florida cited in the ABA opinion at note 7. The South Carolina Ethics Committee has not advised on the issue. If a lawyer is appearing in a matter in another jurisdiction, the rules of the jurisdiction in which the tribunal sits will apply. See SCRPC 8.5(b)(1). Given this split in authority, lawyers should take reasonable precautions to protect from disclosure the metadata in their documents. The ABA committee observed that counsel sending a document could take a variety of steps to avoid revealing metadata, including use of scrubbing programs. Such programs are widely available on the market, and prudent counsel will use one of them before sending a document. Of course, as the ABA committee noted, if the original of a document is demanded in discovery, the lawyer could not ethically scrub the document then if he failed to do so when it was sent, although the lawyer could object to production of metadata that would reveal privileged information. See ABA Opinion 06-422 at n. 13. For a good article on types of metadata and scrubbing techniques, see Robert Brownstone, Metadata: To Scrub Or, Cal. Bar J. (Feb. 2008).

**Loss of flash drives, smart phones, laptops, or other devices**

All of the devices that lawyers use today can be lost, and the smaller the device, the more likely it is to be lost. These devices contain enormous amounts of information, much of which is confidential. Reasonable precautions require law firms to recognize the possibility of loss of devices and to develop appropriate policies to reduce the risk of loss. It would be useless to implement sophisticated protection from digital attacks when the confidentiality of clients can be violated simply by the drop of a flash drive. What precautions should firms consider with these portable devices? For example, a firm could prohibit the use of personal devices on firm matters. Lawyers would be required to use only firm flash drives, PDAs, and laptops that have file encryption, that are password protected, and that contain confidentiality notices with instructions for return on the case of the device. Are these steps ethically required? They might not be, particularly for solo practitioners and small firms where the costs of such steps might be substantial. At a minimum, however, if a lawyer is using a device for both business and personal purposes, the device should be password protected, with a strong password, i.e. one containing both letters, numbers, and at least one character. The more digits the better, of course. I have been told that it takes two minutes for a hacker to discover a four-digit password, but it could take two centuries to identify an eight-digit password. One last point with regard to loss of devices—check to see if your insurance covers cyber loss; you might need to buy a separate policy.

**Disposal of devices**

The number of devices with hard drives that can store confidential client information is enormous, including computers, printers, copiers, scanners, cellular phones, PDAs, flash drives, memory sticks, and facsimile machines. When such devices are disposed of, there is a risk of disclosure of confidential client information. In Opinion 10-2, the Florida Bar Professional Ethics Committee addressed these issues. The committee identified the following specific obligations based on the general duties of confidentiality (SCRPC 1.6), competence (SCRPC 1.1), and supervision (SCRPC 5.3):

(a) inventorying devices that contain hard drives or other storage mechanisms;
(b) supervising nonlawyers, both employees and independent contractors, to make sure they are aware of the confidentiality obligation of lawyers, that they have agreed to comply with those obligations, and that they are taking reasonable steps to comply with that obligation;
(c) assuring that devices are cleansed of confidential information before disposition, either by having this occur at the lawyer's office, by meaningful confirmation, or by some other reasonable means;
(d) keeping abreast of changes in technology to keep current firm policies regarding disposal of devices; and
(e) recognizing that threats to confidentiality could occur with the use of devices located in places other than the lawyer's office, such as copy centers, business centers at hotels, and home offices. The committee advised that lawyers should inquire and determine whether the use of devices at such places poses a threat to confidentiality. ■