

This is the second column dealing with confidentiality issues raised by the use of modern technology in the practice of law. In my last column I examined: (1) public use of technology, (2) metadata in document transmission, (3) loss of devices, and (4) disposal of devices. This article will consider (5) outsourcing and “the cloud,” (6) use of networking sites, and (7) dealing with confidentiality breaches. In this column I also suggest one way of addressing these issues—development of law firm policies 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.

Outsourcing and “the cloud”

Use of “the cloud” is one of the hot issues in the practice of law, but what exactly is the cloud? Imagine a lawyer who works in a firm. The lawyer will use his own computer and will have access to other firm information through a firm intranet. The firm purchases or leases applications from various providers. The concept of the cloud moves the firm’s storage, application acquisition, and application maintenance from beyond the firm to the Internet. Data storage is on remote computers that the firm may not be able to identify easily. Updates of applications become immediately available through the Internet. Any device with an Internet connection regardless of location can access any of the firm’s applications via the Internet. Cloud computing offers a number of possible advantages for lawyers and their firms, including expanded data storage, immediate application updates, greater accessibility, and reduced

cost. Because the cloud involves moving storage of firm data outside the firm to servers of various providers, it obviously poses issues of confidentiality.

A few opinions have examined the ethical propriety of lawyers using cloud computing. In broad terms these opinions have concluded that lawyers may ethically use cloud computing provided they take reasonable precautions to protect client confidentiality. See N.Y. State Bar Op. 842 (2010). As is true with many issues, however, the details are determinative. What steps are lawyers required to take in order to assure reasonable protection of client confidences? The New York opinion provides a useful list. Reasonable care includes:

1. Ensuring that the provider has an enforceable obligation to preserve confidentiality and security, and that the provider will notify the lawyer if served with process demanding client information;
2. Investigating the adequacy of the provider’s security measures, policies, “recoverability methods,” and other procedures;
3. Using available technology to prevent attempts to hack into the stored data;
4. Exploring the provider’s ability to move the data to a different host and purge copies of the data if the lawyer wants to change providers;
5. Periodically reconfirming that the provider’s security measures remain effective in light of advances in technology;
6. Upon learning of any breach of confidentiality by the provider, the lawyer must investigate whether the breach involved the clients’ information, notify any affected clients, and discontinue use of the service unless the security issues are fixed;
7. Monitoring the evolving law relat-

- ing to technology and protection of confidential communications, especially legal developments concerning privilege waiver; and
8. Staying abreast of evolving technology to assess any changes in the likelihood of interception as well as the availability of improved technologies that may reduce such risks at reasonable cost.

This opinion contains both good and bad news. On the one hand, it confirms that use of the cloud is ethically permissible. On the other, it requires lawyers to engage in a level of scrutiny of their providers that may be unfamiliar to many lawyers.

Confidentiality and the use of networking sites

The use of networking sites both for social and professional purposes has boomed in recent years, and lawyers have become active participants in this development. I have written previously on the ethical issues raised by the use of social networking sites. See *Ethical Issues in Using Social Networking Sites*, S.C. Lawyer 8 (November 2009). Whether in physical or electronic form, disclosure of confidential information by lawyers as part of a marketing effort is improper. The *ABA Journal* reported on a case in which a law firm was fined \$25,000 for referring to a \$17 million confidential settlement against a builder when the firm wrote to other homeowners in an effort to persuade them to bring similar litigation. See Martha Neil, *ABA Journal News* (April 16, 2009). The same result would follow if the firm attempted to use the settlement on its website, LinkedIn page, or by e-mail communication. See also S.C. Bar Ethics Adv. Op. #-02-15 (holding that an attorney’s violation of the provisions of a confidential settlement agreement was a reportable

offense under Rule 8.3(a), but the lawyer who had knowledge of the violation was required to obtain client consent under Rule 8.3(c) before reporting because the information related to the representation of the lawyer's client under Rule 1.6(a).

Suppose the information that lawyer wants to use is not subject to a confidentiality agreement. For example, if a lawyer has obtained a favorable judgment from a defendant in a products liability case, the lawyer might wish to publicize the settlement on his website, his LinkedIn site, or on Twitter. Lawyers must remember that the ethical duty of confidentiality is broad. Under Rule 1.6(a) the duty applies to any information "relating to the representation of a client." The duty applies regardless of the form of information—whether oral, written, or electronic—and regardless of the source of the information—whether client, third party, or generated through investigation. The rule does not contain an exception for public information, so merely because the information is part of the public record does

not mean that the duty of confidentiality is inapplicable. In *Sealed Party v. Sealed Party*, 2006 WL 1207732 (S.D. Tex. 2006), a Texas federal district court held that the Texas Rules of Professional Conduct do not provide an exception to the duty of confidentiality to reveal either "public" information or "generally known" information. On the other hand, the Restatement takes the view that "generally known" information is not subject to the duty of confidentiality. Under the Restatement view, information that has been revealed to others remains subject to the duty of confidentiality unless it is generally known. Information about the law, legal institutions, and similar matters is not subject to the duty of confidentiality even though the lawyer may acquire such information while working on a client matter, so long as the lawyer does not otherwise disclose client confidences. Restatement (Third) of the Law Governing Lawyers §59 (2000). The rules of some jurisdictions, such as New York, provide exceptions for widely known public information. In sum, the bot-

tom line is that references to a client or a client's matter without client consent, even when the references are a matter of public record, are risky at best.

Dealing with confidentiality breaches

Many states, including South Carolina, have data security laws. See the website of the National Conference of State Legislature dealing with Security Breach Notification Laws. The South Carolina statute, 39-1-90(A), provides

A person conducting business in this State, and owning or licensing computerized data or other data that includes personal identifying information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of this State whose personal identifying information that was not rendered unusable through encryption, redaction, or other methods was, or is reasonably



At the end of the day...
Who's Really Watching Your Firm's 401(k)?
And, what is it costing you?

- Does your firm's 401(k) include professional investment fiduciary services?
- Is your firm's 401(k) subject to quarterly reviews by an independent board of directors?
- Does your firm's 401(k) feature no out-of-pocket fees?

••••• *If you answered no to any of these questions, contact the ABA Retirement Funds Program to learn how to keep a close watch over your 401(k).*



Who's Watching Your Firm's 401(k)?

Phone: (800) 826-8901

email: contactus@abaretirement.com

Web: www.abaretirement.com



The American Bar Association Members/Northern Trust Collective Trust (the "Collective Trust") has filed a registration statement (including the prospectus therein (the "Prospectus")) with the Securities and Exchange Commission for the offering of Units representing pro rata beneficial interests in the collective investment funds established under the Collective Trust. The Collective Trust is a retirement program sponsored by the ABA Retirement Funds in which lawyers and law firms who are members or associates of the American Bar Association, most state and local bar associations and their employees and employees of certain organizations related to the practice of law are eligible to participate. Copies of the Prospectus may be obtained by calling (800) 826-8901, by visiting the website of the ABA Retirement Funds Program at www.abaretirement.com or by writing to ABA Retirement Funds, P.O. Box 5142, Boston, MA 02206-5142. This communication shall not constitute an offer to sell or the solicitation of an offer to buy, or a request of the recipient to indicate an interest in, Units of the Collective Trust, and is not a recommendation with respect to any of the collective investment funds established under the Collective Trust. Nor shall there be any sale of the Units of the Collective Trust in any state or other jurisdiction in which such offer, solicitation or sale would be unlawful prior to the registration or qualification under the securities laws of any such state or other jurisdiction. The Program is available through the South Carolina Bar as a member benefit. However, this does not constitute an offer to purchase, and is in no way a recommendation with respect to, any security that is available through the Program

C11-0318-012 (3/11)

believed to have been, acquired by an unauthorized person when the illegal use of the information has occurred or is reasonably likely to occur or use of the information creates a material risk of harm to the resident.

A person who violates the statute is subject to liability for damages, including attorney fees. For a knowing and willful violation, a person is subject to a civil penalty of \$1000 for each resident of the state whose information was accessible. The statute only applies to personal identifying information, which is defined as the name of a person in association with some other piece of important information, such as a social security or bank account number. See S.C. Code 16-13-510(D). A law firm that handles cases involving individuals could be required to give notification under this statute in the case of a security breach. The statute would not apply to information about businesses. However, the rules of ethics require lawyers to communicate with their clients. In

particular, Rule 1.4(b) states: "A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation." In my opinion a law firm representing business clients that suffered a security breach would be ethically required to inform its business clients about the breach so that they could make informed decisions regarding the matter.

Provision in engagement agreement

As my two columns have indicated, the use of technology presents a number of confidentiality risks. To deal with these risks, law firms need to adopt appropriate policies and procedures. This column has suggested a number of such protocols. A useful source for developing firm policies and procedures is the regulations adopted by the Massachusetts Department of Consumer Affairs pursuant to the state's data privacy law. See 201 CMR 17.00. These regulations require "Every person that owns or licenses personal information about a resident of the Commonwealth shall develop, implement, and maintain a comprehensive information security program." The regulations go on to provide standards for such a program.

Communication to clients is an important aspect of any data security program. As discussed above, the duty to communicate, in my opinion, requires lawyers to inform their clients of any significant security breach. Communication begins, however, with the engagement agreement. In my opinion law firms should include in their engagement agreements provisions dealing with the use of technology. I offer the following provision for your consideration:

This law firm uses various devices in the representation of clients, including desk top and laptop computers, smart phones, tablets, copy and fax machines, and flash drives. These devices use a number of different applications, including word processing, e-mail, and spreadsheets. The

devices also contain memory in which information is stored. These devices and their applications have increased the efficiency of the practice of law to the benefit of clients. At the same time, the use of these devices, applications, and data storage systems have increased the transmission and storage location of client information, thereby increasing the risk that such information may be compromised. The firm has instituted various policies and procedures to protect the confidentiality of client information. A detailed statement of these policies and procedures is available at —. By signing this engagement you consent to the firm's use of these technologies in accordance with the policies and procedures adopted by the firm. If you have any questions, concerns, or special requests regarding the protection of your confidential information, please discuss the matter with the attorney who is responsible for your case or with —, the managing attorney of the firm.

Recent developments since the last column


Since I wrote the last column at the end of July, the following significant developments have occurred: (1) The ABA's Ethics 20/20 Commission, which is considering revisions to the Model Rules of Professional Conduct, has issued a draft of its proposed revisions to the Model Rules dealing with the ethical issues raised by use of technology. See the website of the ABA Ethics 20/20 Commission. (2) The ABA Committee on Ethics and Professional Responsibility has issued Formal Opinion #11-459, dealing with a lawyer's ethical obligations when the lawyer represents a client who may be using the computer system of the client's employer or some other third party for sending confidential e-mails to the lawyer, and Formal Opinion #11-460, dealing with the ethical obligations of counsel for an employer when counsel receives copies of e-mails sent by the employee to his counsel. ■

BLUESTEIN LAW FIRM, P.A.

S. Scott Bluestein

*Admiralty and
Maritime Law*

Maritime Personal Injury
Boating/Jet ski Accidents
Cargo Damage
Recreational Boats
Vessel Arrests
Marine Insurance Claims
Seamen Claims



1040 eWall Street
Mt. Pleasant, SC 29464
Email: boatinglaw@bellsouth.net
(843) 577-3092 Fax: (843) 577-3093
www.bluesteinlawoffice.com