September 2010 *Multnomah Lawyer Ethics Focus*

Up in the Air:
Cloud Computing and Confidentiality

By Mark J. Fucile
Fucile & Reising LLP

Wikipedia defines "cloud computing" as "Internet-based computing, whereby shared resources, software and information are provided to computers and other[s] . . . on-demand." Commercial applications of cloud computing are many, but one emerging trend among law firms is Web-based file storage. In this setting, law firms store and access files (both electronically created documents and imaged copies that were originally in paper form) on remote servers managed by independent vendors. Some firms use electronic storage as back-up, some as a primary means of accessing documents and some do both. The economic driver is the potentially lower cost associated with electronic rather than paper storage. The technological driver is the ability to access files virtually anywhere.

While offering innovative solutions to file management, this application of "cloud computing" also presents new challenges to protecting client confidentiality. Off-site file storage, of course, is nothing new. Law firms have long used commercial vendors for off-site storage of paper files—typically closed files that have been archived. The confidentiality issues are nothing new either. In fact, the ABA has a series of ethics opinions dating back over 20 years on outsourced services generally and computer data bases in particular (*see, e.g.,*

ABA Formal Ethics Op 95-398). Oregon, too, has dealt with outsourcing in the file management context (*see, e.g.*, OSB Formal Ethics Op 2005-141). Still other states have addressed Web-based file storage and retrieval specifically, including Arizona (Ethics Op 09-04), New Jersey (Opinion 701), Nevada (Ethics Op 33) and North Carolina (2008 Formal Ethics Op 5).

Both the opinions addressing outsourcing generally and those examining Web-based file storage specifically weave together two concepts that are neatly captured in the heading to a key section of the comments to ABA Model Rule 1.6, the confidentiality rule: "Acting Competently to Preserve Confidentiality." We have a general duty under RPC 1.1 of competent representation. We also have a general duty under RPC 5.3 to supervise nonlawyers who assist us. One element of these general duties is protecting client confidentiality. With electronic files, our duty to "act competently to preserve confidentiality" applies to both storage and transmission.

Storage

Comment 16 to ABA Model Rule 1.6, upon which Oregon's corresponding rule is patterned, highlights our role in choosing a storage provider with security measures consistent with our own duty to protect confidentiality:

> "A lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision."

The ethics opinions on outsourcing generally and those dealing with Web-based storage specifically discuss competence in this sense as the reasonable investigation, selection and monitoring of a storage provider to make sure that the provider understands the lawyer's duty of confidentiality and has protections in place consistent with that duty. With paper file storage, the focus is typically on physical security. With electronic files, physical security at the data center is equally important. But, precisely because the information is in electronic form, protection from "unauthorized access" extends to reasonable electronic security measures as well. What is "reasonable" will vary with the circumstances, but includes the electronic equivalent of a secure "lock and key" to Web access.

Transmission

Comment 17 to ABA Model Rule 1.6 addresses the need to maintain confidentiality when transmitting information and, in doing so, has particular application to electronic files:

> "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. 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."

One of the principal advantages of electronic storage is that files are readily accessible via the Web. That, in turn, puts a premium on ensuring that the means chosen for access is secure. Federal law prohibiting the unauthorized interception of (*see, e.g.*, Electronic Communications Privacy Act) or the unauthorized intrusion into (*see, e.g.*, Stored Communications Act) electronically transmitted data provides a baseline "reasonable expectation of privacy." Again depending on the circumstances, however, encryption or other special data security measures may be warranted.

Summing Up

It often makes sense to outsource the logistical functions of law practice. It is equally important to remember, however, that we cannot "outsource" our responsibility for protecting client confidentiality.

ABOUT THE AUTHOR

Mark J. Fucile of Fucile & Reising LLP focuses on legal ethics, product liability defense and condemnation litigation. In his legal ethics practice, Mark handles professional responsibility, regulatory and attorney-client privilege matters and law firm related litigation for lawyers, law firms and legal departments throughout the Northwest. He is a past member of the Oregon State Bar's Legal Ethics Committee, is a past chair of the Washington State Bar Rules of Professional Conduct Committee, is a member of the Idaho State Bar Professionalism & Ethics Section and is a co-editor of the OSB's Ethical Oregon

Lawyer and the WSBA's Legal Ethics Deskbook. Mark also writes the monthly Ethics Focus column for the Multnomah (Portland) Bar's Multnomah Lawyer, the quarterly Ethics & the Law column for the WSBA Bar News and is a regular contributor on risk management to the OSB Bar Bulletin, the Idaho State Bar Advocate and the Alaska Bar Rag. Mark's telephone and email are 503.224.4895 and Mark@frllp.com.