fucile & reising | LLP

July-August 2012 *Multnomah Lawyer Ethics Focus*

Cloud Computing: Confidentiality and Coverage

By Mark J. Fucile
Fucile & Reising LLP

Lawyers have used off-site storage for a long time. Traditionally, "off-site storage" meant a physical location (ranging from professionally managed facilities to individual storage units) where lawyers stored their closed files. More recently, "off-site storage" has evolved into "cloud computing" where documents are stored electronically on remote servers managed by independent vendors and accessed via the Web. 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 an innovative solution to file management, this application of "cloud computing" also presents new challenges to protecting client confidentiality—especially when the storage sites involved are being managed by independent vendors. The Oregon State Bar addressed these issues last year in Formal Ethics Opinion 2011-188. The Professional Liability Fund, in turn, created an exclusion for associated data loss earlier this year. In this column, we'll look at both confidentiality and coverage.

Confidentiality

The new ethics opinion weaves 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 duties under RPC 1.1 and 1.6 to, respectively, competently represent our clients and to protect their confidentiality both during and after a representation. Further, although we can use nonlawyers to assist us, we have a duty under RPC 5.3 to adequately supervise them so their work will be consistent with our ethical and fiduciary obligations.

Opinion 2011-188 emphasizes (at 2) that although we can delegate the technical task of storage to an appropriately qualified vendor, we cannot delegate the ultimate responsibility for protecting client confidentiality:

> "Lawyer may store client materials on a third-party server so long as Lawyer complies with the duties of competence and confidentiality to reasonably keep the client's information secure within a given situation. To do so, the lawyer must take reasonable steps to ensure that the storage company will reliably secure client data and keep information confidential."

Opinion 2011-188 also emphasizes (at 3) that the duty to evaluate the adequacy of a vendor's security measures is dynamic rather than static:

> "Although the third-party vendor may have reasonable protective measures in place to safeguard the client materials, the reasonableness of the steps taken will be measured against the technology 'available at the time to secure data against unintentional disclosure.' As technology advances, the third-party vendor's protective measures may become less secure or obsolete over time. Accordingly, Lawyer may be required to

> reevaluate the protective measures used by the third party vendor to safeguard the client materials."

Coverage

Although cloud computing offers both convenience and accessibility, it also comes with a risk that we are becoming all too familiar with in a wide variety of contexts: hacking and associated data theft. In response, the PLF amended its base policy this year to add a specific exclusion—Exclusion 22—for data loss:

> "This Plan does not apply to any CLAIM arising out of or related to the loss, compromise or breach of or access to confidential or private information or data. If the PLF agrees to defend a SUIT that includes a CLAIM that falls within this exclusion, the PLF will not pay any CLAIMS EXPENSE relating to such CLAIM."

The accompanying comments note that Exclusion 22 applies to both electronic and traditional storage. In announcing the new exclusion, the PLF stressed that this is a problem that malpractice carriers are grappling with nationally and that it is searching for a solution appropriate for Oregon practice. In the meantime, however, firms not otherwise covered through a general liability or excess policy that includes such coverage will need to balance the utility of off-site storage with the corresponding risk.

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.