The Ethics of Cloud Computing and Storage

So-called "cloud computing" includes any software and hardware package that allows a lawyer to transmit, manipulate, store, and retrieve data off the lawyer's premises - in the proverbial clouds - rather than on the hard drive seated on the lawyer's desk. It includes platforms like web-based e-mail, online data storage, software-as-a-service ("SaaS"), platform-as-a-service ("PaaS"), infrastructure-as-a-service ("IaaS"), Amazon Elastic Cloud Compute ("Amazon EC2"), and Google Docs to name a few examples.

While the technology is perpetually renewing and reinventing itself, cloud computing triggers the same ethical obligations that lawyers always have owed to their clients. Think of it like a roadway intersection that is re-engineered and reconstructed to improve the flow of traffic. The number of lanes may increase, the roadway markings may change, and the traffic control devices may be new, but the rules of the road for approaching vehicles remain the same for that intersection as for any outdated intersection. With the expansion of remote data storage and processing services, or cloud computing, comes the need to observe the same, previously established ethical obligations attorneys always have followed in caring for client information.

Commentators on the ethics implications of cloud computing generally identify several current rules of professional conduct affected by the new technology, such as Rule 1.1 (competence), Rule 1.4 (communications with client), Rule 1.6 (confidentiality), Rule 1.15 (safeguarding client property), and Rule 5.3 (supervision of third parties).

With the shift from paper hardcopies to electronic data, the Maine Professional Ethics Commission issued Opinion #183 on January 28, 2004. The Opinion answered the question whether an attorney is obligated to keep a paper copy of correspondence if that correspondence is converted to an electronic format and stored on a computer. Analyzing then applicable Rules 3.5(a) and 3.6(a) & (e) and Opinions #74 & #120, the Commission concluded that the ethics rules did not require the attorney to retain a paper copy in addition to the electronic one but only under certain conditions. Those conditions generally ensured that the electronic format did not make the correspondence any less accessible to the client than a paper document. Rule 3.5(a) exists today within the current Rules of Professional Conduct 1.15(f) and 1.16(d), and the 2004 Rule 3.6(a) & (e) have carried over into Rules 1.1, 1.3, 1.4, and 1.15(a) & (f). Note, however, that Rule 1.15(f) states that there is an obligation now to retain and safeguard client records that have "intrinsic value in the particular version, such as original signed documents," rather than destroy them after conversion to an electronic format.

In 2008, the Commission came close to addressing the ethics of what currently is known as cloud computing. Opinion #194 discussed the ethical propriety of using third-party vendors to process and store electronic data comprised of the client's file. The scenario posed included transmitting electronic recordings - presumably the lawyer's dictated correspondence, briefs and the like about the client's confidential information - for off-site transcription and transferring client files in the form of the electronic data off-site for backup storage. The Commission relied on then Rules 3.6(a) & (h) and 3.13(c), as well as Opinions #74 & #134, to come to the conclusion that
"with appropriate safeguards, an attorney may utilize transcription and computer server backup services remote from both the lawyer's direct control or supervision without violating the attorney's ethical obligation to maintain client confidentiality." The 2008 version of Rule 3.6(a) & (h) can be found in the current Rules 1.1 and 1.6, and then Rule 3.13(c) translates to current Rule 5.3.

What changes with evolving technology like cloud computing is not the overriding ethical constraints on counsel, but how those constraints are satisfied with respect to new challenges presented by the technology. What must the lawyer do to provide reasonable and enforceable assurances that the third-party vendor will protect client confidences? How does the lawyer confirm the destruction of data held by the vendor when the client file is closed? Can the lawyer retrieve client files if the vendor closes its business? A full discussion of how an attorney complies with the specific ethics rules implicated as to a particular proprietary "cloud" product is beyond the scope of this article. Ethics commissions in other jurisdictions and legal scholars have written extensively on the nuts and bolts of acting ethically in the cloud, including providing checklists. See, e.g., Pennsylvania Formal Opinion 2011-200; North Carolina 2011 Formal Opinion #6 (January 27, 2012); and The American Bar Association, "Ethical Challenges on the Horizon: Confidentiality, Competence, and Cloud Computing," 2012.