



Law Firms and Cloud Computing

December 28, 2012

The term “cloud computing” has been tossed about as the new trend in IT. Unfortunately, just as often have you hear the term echoed as the “next big thing” a comprehensible definition rarely follows. So what is cloud computing? The United States National Institute of Standards and Technology (“NIST”) defines cloud computing as:

A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

Perhaps more succinctly put, cloud computing “involves the sum of a service to store, transmit and process information and employs the internet as the means to access and move the information.” ^[1]

How does contracting with a cloud service provider impact confidential information that is shared with the third party? *American Bar Association Model Rule 1.6* requires lawyers to maintain all information relating to client representation in confidence. ^[2] Under *Model Rule 1.6* an attorney must take “reasonable precautions” to guard against inadvertent disclosure. The exact formulation of what constitutes “reasonable precautions” is never provided; rather, the reasonableness of a precaution is a fact-sensitive analysis. *Id.* An attorney must consider the risk of harm, the likelihood of disclosure, and the extent to which the privacy of the communication is protected by either law or **confidentiality agreement**. *Id.*

In *Warshak v. United States* 490 F.3d 455, 473 (6th Cir. 2007), the Court offered some guidance as to what constitutes appropriate precautions when dealing with a third party cloud service. The Court reasoned that a key component in maintaining a reasonable expectation of privacy is the assurance from the third party host that the data “provided” will neither be monitored nor audited. ^[3]

In September of 2010, the New York State Bar Association’s Committee on Professional Ethics released Opinion 842. Opinion 842’s topic was “using an outside online storage provider to store client confidential information.” Opinion 842’s digest states that:

A lawyer may use an online data storage system to store and back up client confidential information provided that the lawyer takes reasonable care to ensure that confidentiality will be maintained in a manner consistent with the lawyer’s obligations under Rule 1.6. In addition, the lawyer should stay abreast of technological advances to ensure that the storage system remains sufficiently advanced to protect the client’s information, and

should monitor the changing law of privilege to ensure that storing the information online will not cause loss or waiver of any privilege.

In addition, Opinion 842 provides that an attorney must also exercise reasonable care in preventing “others whose services are utilized by the lawyer from disclosing or using confidential information of a client.” This requires affirmative steps to guard against inadvertent disclosure. The New York State Bar Association has summed up advisory opinions from several other jurisdictions finding that sufficient precautions must be in place when using electronic storage of client files.

New Jersey Opinion 701 (2006) (**lawyer may use electronic filing system whereby all documents are scanned into a digitized format and entrusted to someone outside the firm provided that the lawyer exercises “reasonable care,” which includes entrusting documents to a third party with an enforceable obligation to preserve confidentiality and security**, and employing available technology to guard against reasonably foreseeable attempts to infiltrate data); Arizona Opinion 05-04 (2005) (electronic storage of client files is permissible provided lawyers and law firms “take competent and reasonable steps to assure that the client’s confidences are not disclosed to third parties through theft or inadvertence”); *see also* Arizona Opinion 09-04 (2009) (lawyer may provide clients with an online file storage and retrieval system that clients may access, provided lawyer takes reasonable precautions to protect security and confidentiality and lawyer periodically reviews security measures as technology advances over time to ensure that the confidentiality of client information remains reasonably protected).

NYSBA Opinion 842 (emphasis added)

For more information regarding the use of cloud computing in law firms, contact Arturo Castro, an associate at Cullen and Dykman. Arturo can be reached at acastro@cullenanddykman.com.

1. ^[1] Peter M. Lefkowitz, *Department: Practice Tips: Contracting in the Cloud: A Primer*. 54 B.B.J. (Boston Bar Journal) 9.
2. ^[2] Shellie Stephens, *Recent Development: Going Google: Your Practice, the Cloud, and the ABA Commission on Ethics 20/20*, 2011 U. Ill. J.L. Tech and Pol’s (University of Illinois Journal of Law, Technology, and Policy) 237.
3. ^[3] Shellie Stephens, *Recent Development: Going Google: Your Practice, the Cloud, and the ABA Commission on Ethics 20/20*, 2011 U. Ill. J.L. Tech and Pol’s (University of Illinois Journal of Law, Technology, and Policy) 237.