ETHICS for Lawyers and Law Firms Using Cloud Technology

Donna Kirk Seyle ~ Legal Tech Advisor: Law Practice Strategy
108 MONTESANO ST | SANTA CRUZ, CA 95062 | (831) 332-2243

Donna Seyle is an attorney, author, and Founder of Law Practice Strategy, where she advises lawyers and law firms on the use and integration of legal cloud technology to expand their legal service delivery options, and offers unique content marketing and publishing services. LPS also provides real-time information on the future of law practice and emerging legal business models.

Donna is a member of the ABA-LPM's eLawyering Task Force, which explores tech innovation and its impact on the profession, and using these advances to improve access to justice. She also serves as a member of the State Bar of California - Law Practice Management & Technology Section Executive Committee, where she chairs several sub-committees.

Donna is the author of Law Practice Strategy: Creating a New Business Model for Solos and Small Firms (available on Amazon), as well as the virtual law practice section of the State Bar of California’s new book, The California Guide to Growing & Managing a Law Office.

Ms. Seyle graduated from Southwestern University School of Law, Los Angeles, in 1986, and practiced Real Estate law. In 2008, she became involved in social media and the legal technology community, attending major legal tech conferences, researching the future of law as affected by technology, and interacting with many internationally thought leaders in the area. She brings all of this knowledge to bear on her efforts to educate lawyers on the process of integrating cloud technology into their practices.

DISCLAIMER: The following materials and accompanying Access MCLE, LLC audio program are for instructional purposes only. Nothing herein constitutes, is intended to constitute, or should be relied on as, legal advice. The author expressly disclaims any responsibility for any direct or consequential damages related in any way to anything contained in the materials or program, which are provided on an “as-is” basis and should be independently verified by experienced counsel before being applied to actual matter. By proceeding further you expressly accept and agree to Author’s absolute and unqualified disclaimer of liability.
Table of Contents

INTRODUCTION ........................................................................................................................................ 3
M.R. Confidentiality: Rules 1.6(a) and 1.15 .......................................................................................... 3
M.R. Competence and Diligence: ........................................................................................................... 5
Rules 1.1 and 1.3, cited by California Rule 3-110 ............................................................................... 5
M.R. Duties to Prospective Clients: Rules 1.18 and 1.2 ...................................................................... 6
M.R. Unauthorized Practice of Law: Rule 5.5 ....................................................................................... 7
M.R. Duty to Supervise: Rule 5.3 ........................................................................................................... 8
State Bar Formal Opinions .................................................................................................................... 8
Summary .................................................................................................................................................. 9
Online Resources for Legal Ethics and Cloud Computing ................................................................. 10
INTRODUCTION

The importance of ethical considerations in using cloud technology in your law practice cannot be overstated. Yet, it is one of the most misunderstood areas of regulation with which lawyers are mandated to comply. There are good reasons for this state of affairs: IT-aholics develop new software, and new iterations of this new software, faster than anyone can keep up with. And of course, the legal profession and those who regulate it showed up late to the dance.

That said, the last two years have seen the American Bar Association and State Bar Associations playing catch-up. There has been an increasing number of Model and State Bar Rule revisions and clarifications that address the issues lawyers need to be cognizant of, and the procedures they should integrate into their practices in response to the potential for harm to their clients when using cloud technology.

This document is a focused review of the Model and California Rules related to two distinct areas of cloud use by lawyers:

- the use of cloud technology in performing their work as lawyers
- the use of social networking and internet advertising and solicitation

M.R. Confidentiality: Rules 1.6(a) and 1.15

The duties of confidentiality and to safeguard client property come into play when confidential client information is transmitted and/or stored in a cloud-based system, and with almost all uses of cloud computing by lawyers, from email to online delivery of legal services. The underlying risk is loss of control of your data and communication that is being transmitted and/or stored by a third-party vendor.

Comment 17 to Rule 1.6(a) provides that lawyers must take “reasonable precautions” to safeguard confidential information and prevent it from going to unintended recipients during transmission. Rule 1.6(a) sets the standard for safeguarding client property, but begs the question of what constitutes “reasonable precautions.” Lawyers are also responsible to stay current with developments in the technology they use.

Most states are adhering to a “reasonable care” standard in determining whether a lawyer has done his or her duty to protect client confidentiality when using cloud computing. If the lawyer does not feel that she understands how to make these decisions, then she is expected to retain the services of an IT consultant who may assist them in the due diligence process. The primary duty in this process is to vet the cloud vendor before contracting with them. This will be discussed further below.
Whether an attorney violates her duties of confidentiality and competence (see below) when using technology to transmit or store confidential client information depends on the technology they are using, and the circumstances surrounding their use. Before using a particular technology when representing clients, an attorney must take appropriate steps to evaluate:

- The level of security attendant to the use of that technology, and whether reasonable precautions should be taken when using the technology to increase the level of security;
- The legal ramifications to a third party who intercepts, accesses or exceeds authorized use of the electronic information (if a third party could be subject to civil or criminal charges, the client’s expectation of privacy is deemed greater);
- The degree of sensitivity of the information;
- The possible impact on the client of an inadvertent disclosure of privileged or confidential information or work product;
- The urgency of the situation;
- The client’s instructions and circumstances, such as access by others to the client’s devices and communications.

Attorneys should keep in mind that this is a very ‘location-based’ opinion. The Bar is asking attorneys (and support staff) to be aware of not only their surroundings, but whether their communications are as confidential as if they were sitting in a formal setting behind a firewall. In other words, if one is sitting at an airport, one must rely on one’s own firewall (including via wireless devices like smart-phones and tablets). Furthermore, can the person sitting next to the attorney/staff see their screen while they’re working on confidential client information?

Remember: The attorney is subject to a Duty to Supervise (See #5, M.R. 5.3)
M.R. Competence and Diligence:

Rules 1.1 and 1.3, cited by California Rule 3-110

The duty of competence is defined to include taking appropriate steps to ensure both that secrets and privileged information of a client remain confidential and that the attorney’s handling of such information does not result in a waiver of any privileges or protections.

Under both the Model and California Rules, the duties of competence and diligence, when applied to cloud computing, require lawyers to do the following:

- understand the technology and security issues when selecting a cloud service provider and devices;
- conduct due diligence in vetting their chosen vendor;
- diligently follow best practices in the daily management and use of the technology to insure confidentiality;
- inform clients of their use of cloud software in the act of representation;
- best practices require lawyers to use cloud computing to conduct factual research in the proper representation of their client.

Vetting your chosen vendor is essential to make certain the software uses security practices sufficient to enable you to meet your ethical obligations. Here is a list of questions to ask when conducting this aspect of due diligence:

- Where are the primary servers located?
- Where are the back-up servers located?
- Are there redundant power supplies for the servers?
- How often, and in what manner, is users’ data backed up?
- What are the regulatory requirements in the jurisdiction where the servers are located?
- Do they engage in cross-jurisdictional or cross-border data transfers? If so, when and where? Will you be notified?
- Is there a compliance plan for cross-jurisdictional or cross-border transfers?
- Do they employ Tier 4, 256-bit encryption, bank-level security?
- What types of encryption methods are used and how are passwords stored?
- How are passwords protected?
- Are these security measures in place both while the data is in transition and in storage?
- Have their operations ever been audited? (If so, obtain a copy of the report).
- What is their annual server uptime? (Obtain a copy of the report for as many years as possible).
• Do they own their servers, or lease them from a 3rd-party?
• If they lease them, what are the terms of the 3rd-party agreement? (Obtain a copy).
• Will your data be stored on a dedicated server, or on a multi-tenancy server?
• If multi-tenant, how is your data segregated from others?
• How is the server building physically secured?
• What is their policy regarding employee access to stored data?
• What kind of training is provided their employees?
• Have they ever had a security breach?
• What is their customer notification policy upon breach?
• What is their response policy upon breach?
• What is their disaster recovery/business continuity plan?
• What is their protocol concerning access to and exportation of your data?
• What is the company’s history—e.g., how long have they been in business, and where do they derive their funding?
• Are they Safe-Harbor certified? (Insures that their security measures comply with the EU Directive, a comprehensive regulatory scheme). Not necessary, but comfortable.
• Ask for a copy of their Service Level Agreement (SLA) to review.
• How do they respond to 3rd-party subpoenas?
• Do they attempt to claim full/shared ownership of your data upon transfer to their facilities?
• Do they carry Cyber Insurance to cover losses resulting from a data breach, including 1st-party and 3rd-party coverage?

**M.R. Duties to Prospective Clients: Rules 1.18 and 1.2**

In the world of instant and continuously communication via the internet, questions related to whether someone a lawyer communicates with is a client, when he became a client, and the lawyer’s scope of services often arise. Comment 2 to M.R. 1.18 states that a client is not “a person who communicates information unilaterally to a lawyer, without any reasonable expectation that the lawyer is willing to discuss the possibility of forming a client-lawyer relationship.” That said, Comment 3 provides that the lawyer has a duty to keep the information transmitted confidential regardless of how brief the consultation.” (But see, Barton v. U.S.Dist. Court for the Central Dist. Of Cal., 410 F.3d 1104 (9th Cir. 2005), holding that the attorney/client relationship was formed and a duty of confidentiality arose when prospective clients filled out an online form that the law firm had posted on its website.)

This issue can be addressed by the use of multiple clickwrap agreements and communications with the prospective client, which require that he acknowledge and agree to the terms of use of
cloud technology. It is also the lawyer’s responsibility to define the scope of representation following an initial online consultation.

Present the scope of representation or decision to decline representation to the online client. If the client accepts your services, he is required again to acknowledge that he has notice of this arrangement and is agreeing to it through a tailored clickwrap agreement. The agreement should include the following:

- Notice of the jurisdiction in which the lawyer is licensed to practice law;
- Nature of unbundled or limited scope services (if applicable);
- How and when the attorney/client relationship and scope of representation will be defined;
- Confidentiality policy;
- E-mail policy;
- Site security.

**M.R. Unauthorized Practice of Law: Rule 5.5**

This issue arises with the use of cloud computing when establishing a multijurisdictional virtual law practice and when providing clients with self-help software solutions such as document assembly and self-help services. Lawyers should be clear when creating an online presence about where they are licensed to practice, and provide adequate notice to prospective clients about the jurisdictional limitations of their practice.

Included in the use of cloud technology is the potential for creating “continuous and systematic presence” in a jurisdiction. Comment 4 of M.R. 5.5(d)(3) covers when such presence is established in a jurisdiction by a lawyer who is not admitted to practice there. Comment 4 states: “a lawyer may direct electronic or other forms of communications to potential clients in this jurisdiction and consequently establish a substantial practice representing clients in this jurisdiction, but without a physical presence here. At some point, such a virtual presence may become systematic and continuous within the meaning of Rule 5.5(b)(1).”

While “precision in this area is not possible” and cannot “clearly define the line between a permissible temporary practice...and impermissible systematic and continuous presence, the new additions to Comment 4 provide more guidance to lawyers who create technology-driven legal services that cross geographic boundaries.

Another source of jurisdictional conflict can arise related to a potential client’s residency. Jurisdictional checks should be instituted, upon initial registration, for all prospective clients to
determine a client’s residency. This can best be accomplished by performing an online search for the client.

**M.R. Duty to Supervise: Rule 5.3**

Lawyers who use the services of a legal process outsourcing agency (LPOs), virtual paralegal or assistant or other non-lawyer services are required to make reasonable efforts to ensure their conduct is compatible with the professional obligations of the lawyer. This is all the more important when a retained non-lawyer is given access to the lawyer’s cloud applications.

In order to comply with their supervisory obligations, lawyers should conduct extensive conflicts checks and have confidentiality agreements signed. Supervision over nonlawyers through the use of cloud technology requires the use of a permissions-based system, and they should be given a copy of the firm’s policy for use of cloud software and social media.

**State Bar Formal Opinions**

**The New York State Bar Association** Committee on Professional Ethics concluded in Opinion 842 (Sept. 10, 2010) that the reasonable care standard for confidentiality should be maintained for online data storage and a lawyer is required to stay abreast of technology advances to ensure protection. Reasonable care may include: (1) obligating the provider to preserve confidentiality and security and to notify the attorney if served with process to produce client information, (2) making sure the provider has adequate security measures, policies, and recoverability methods,

**The Alabama State Bar** Office of General Council Disciplinary Commission issued Ethics Opinion 2010-02, concluding that an attorney must exercise reasonable care in storing client files, which includes becoming knowledgeable about a provider’s storage and security and ensuring that the provider will abide by a confidentiality agreement. Lawyers should stay on top of emerging technology to ensure security is safeguarded. Attorneys may also need to back up electronic data to protect against technical or physical impairment, and install firewalls and intrusion detection software.

**State Bar of Arizona** Ethics Opinion 09-04 (Dec. 2009) stated that an attorney should take reasonable precautions to protect the security and confidentiality of data, precautions which are satisfied when data is accessible exclusively through a Secure Sockets Layer (“SSL”) encrypted connection and at least one other password was used to protect each document on the system. The Opinion further stated, “It is important that lawyers recognize their own competence limitations regarding computer security measures and take the necessary time and energy to become competent or alternatively consult experts in the field.” *Id.* Also, lawyers should ensure reasonable protection through a periodic review of security as new technologies emerge.
Massachusetts Bar Association Ethics Opinion 05-04 (March 3, 2005) addressed ethical concerns surrounding a computer support vendor’s access to a firm’s computers containing confidential client information. The committee concluded that a lawyer may provide a third-party vendor with access to confidential client information to support and maintain a firm’s software. Clients have “impliedly authorized” lawyers to make confidential information accessible to vendors “pursuant to Rule 1.6(a) in order to permit the firm to provide representation to its clients.” Id. Lawyers must “make reasonable efforts to ensure” a vendor’s conduct comports with professional obligations. Id.

Pennsylvania Bar Association Committee on Legal Ethics and Professional Responsibility

Ethical Obligations for Attorneys Using Cloud Computing/Software as a Service While Fulfilling the Duties of Confidentiality and Preservation of Client Property

Formal Opinion 2011-200

I. Introduction and Summary

If an attorney uses a Smartphone or an iPhone, or uses web-based electronic mail (e-mail) such as Gmail, Yahoo!, Hotmail or AOL Mail, or uses products such as Google Docs, Microsoft Office 365 or Dropbox, the attorney is using “cloud computing.” While there are many technical ways to describe cloud computing, perhaps the best description is that cloud computing is merely “a fancy way of saying stuff’s not on your computer.”

Summary

The security of online functions used by attorneys to communicate and collaborate with their clients is of major concern to regulatory authorities, one of the subjects of the ABA’s Ethics 20/20 Commission’s review of the Model Rules, and at the core of your ethical obligations to insure the privacy of client data, attorney/client confidentiality and maintenance of the attorney/client privilege.

Recently, the United States District Court in West Virginia held that a bank president who emailed his attorney via the company’s email system waived his attorney/client privilege, where the company’s email policy dictated that all emails sent through their account were considered company property. That is only one of many scenarios that can lead to violations of ethical conduct or waiver of privilege when using online communication tools that are not properly securitized. Use of a client portal is the answer to this challenge.
The eLawyering Task Force is conducting a comparative analysis and study of the various features offered by legal vendors who include client portals in the structure of their SaaS products. The analysis is scheduled to be published in 2012. We are soliciting input from the legal vendors in the industry. The Task Force has also published a set of best practices for law firms that want to deliver legal services based on the concept of the “client portal” application. See: Guidelines for the Use of Cloud Computing in Law Practice from eLawyering Task Force, Law Practice Management Section of the American Bar Association.

In an article in the September Issue of Law Practice Magazine, on predictions for the next five years of eLawyering, Richard Granat and Marc Lauritsen stated that:

“Larger law firms have been using extranet technologies for years, but few solos and small firm practitioners have incorporated client portals into their websites. Recently, however, the cost of this technology has come within reach of even the smallest firms. Think of a personalized web space for each client, giving the firm an online platform for offering a wide range of functions that ordinarily would be provided by telephone, fax, snail-mail or in-person meetings. We predict that within five years almost all law practices will use such a portal.”

Online Resources for Legal Ethics and Cloud Computing

1. Unauthorized Practice of Law in the 21st Century from Topics in Digital Law Practice MOOC 2012, by Will Hornsby
2. Legal Ethics Considerations for Lawyers Use of Cloud Computing Services from Internet for Lawyers by Carol Levitt and Mark Rosch
3. Virtual Lawyering and Virtual Presence under Model Rule 5.5 (b) (1) from eLawyering Redux, by Richard Granat
4. Cloud Ethics Opinions Around the U.S., from ABA’s Legal Technology Resource Center
5. eLawyering in the Age of Accelerating Technology, from ABA’s GP-Solo eReport, by Donna Seyle