

December 15, 2010

Natalia Vera
ABA Center for Professional Responsibility
321 North Clark Street
15th Floor
Chicago, IL 60654-7598

RE: For Comment: Issues Paper Concerning Client Confidentiality and Lawyers' Use of Technology

To whom it may concern,

Thank-you for considering the comments and feedback of the legal technology community as part of your commission's assessment of cloud computing as it relates to client confidentiality.

We are the Legal Cloud Computing Association (LCCA), a consortium of leading cloud computing providers. The founding membership of the LLCA includes Clio (Themis Solutions Inc.), DirectLaw, Inc., Rocket Matter LLC, and Total Attorneys, LLC. The LCCA's charter is to:

- provide a unified and consistent voice for vendors in the legal cloud computing market;
- collaborate and cooperate with Bar Associations and other policy-forming bodies in efforts to form policies and guidelines relating to the use of cloud computing in law practices;
- to define standards and best practices; and
- to provide educational resources to attorneys and the broader legal community on cloud computing and the technical, legal and ethical issues relating to cloud computing.

The LCCA includes in its membership leading experts on cloud computing, data security, privacy and ethics. Our goal is to build a close working relationship with the Commission, and to play a key role in helping build and shape standards, best practices, and education resources for the legal cloud computing market.

The LCCA supports the committee's efforts to provide clarity to its membership on the ethical implications of technologies available via the internet, and appreciates the opportunity to be a part of this important discussion. We firmly believe that many cloud-based solutions are uniquely able to provide a secure, confidential, convenient, and cost-effective method for law firms of any size to manage and store client data, and hope our comments will prove valuable in helping to establish the technical standards that constitute reasonable care when employing Cloud-based solutions.

In this letter we suggest the following for the committee's consideration:

1. Desired form of the Committee's Recommendations
2. Minimal Set of Technology Standards for Cloud Computing Providers
3. Model Terms of Service for Cloud Computing Providers
4. Is Cloud Computing Outsourcing?
5. Cloud Computing Security vis-à-vis E-mail Security

1. Desired Form of the Commission's Recommendations

The LCCA's desired form for the Commission's recommendations would be the creation of an online educational resource for attorneys. This website would be a continually evolving and up-to-date resource providing:

- Overviews of fundamental concepts and terminology relating to cloud computing
- Best practice guidelines
- Articles highlighting recent developments in cloud computing
- Links to relevant ABA and state bar-level ethics opinions and best practice guidelines

We strongly discourage the Committee from contemplating a change to the Model Rules of Professional Conduct as part of its efforts. In their current form, the Rules of Professional Conduct provide a clear, technology-neutral description of an attorney's obligations to maintaining client confidentiality. In many ways, the discussion of security, privacy, ethics and client confidentiality in the era of cloud computing echoes the debate we saw in the 1990s of the same issues as they relate to e-mail. Much of the e-mail security and privacy discussion centered on the obligations outlined by Comment 17 of Rule 1.6 in the ABA Model Rules of Professional Conduct (Client-Lawyer Relationship, Confidentiality of Information):

“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.”

For attorneys to make informed decisions on what “reasonable precautions” entail, and what technologies afford a “reasonable expectation of privacy”, we believe attorneys need to have access to resources that educate with an aim of leaving attorneys in a position to make informed technology decisions.

2. Minimal Set of Technology Standards for Cloud Computing Providers

Here we propose a minimal set of standards by which any cloud computing solution used by any size or type of law firm can be evaluated. These minimal standards collectively form a baseline for the secure storage and transmission of confidential client data across a variety of professional industries that employ cloud computing technology. These minimal set of standards could be incorporated into any recommendations the Commission chooses to make with respect to best practices and cloud computing.

Rule 1.6 of the Rules of Professional Conduct detail the lawyer's duty to protect and preserve the confidences of a client and to ensure any third parties entrusted with confidential data take reasonable measures to minimize the risk that confidential information might be disclosed. The

measures outlined below provide a foundation of security that ensure a lawyer utilizing cloud computing is compliant with Rule 1.6.

Secure Data Centers

One of the most important layers of security for cloud computing providers is the physical security of the data centers that store client data. The following measures help ensure physical access to confidential data is restricted to those with authorized access:

- 24-7 Security monitoring at Data Centers where servers are located
- Access to physical machines is limited only to team responsible for servers
- Machines accessible only through security checkpoints and restricted access areas
- Compliance with relevant standards, such as AICPA SAS 70 Type II¹, PCI² or HIPAA³

Network Security

In addition to being secured against physical compromise, data centers must be adequately protected against network-based threats. The following measures help ensure only approved protocols and connections can be used to access confidential data:

- Perimeter firewalls block unauthorized connections and protocols
- Regular third-party audits of perimeter firewall security

Software Security

Ensuring a data center's software is up-to-date helps protect against known security holes. The following measures help ensure a data center's software is up-to-date:

- Regular, independent audits of software security
- Security patches and software updates applied within 30 days of being published

Data Transmission Security

The previous safeguards help ensure data is securely stored at the data center, but the data must somehow be securely transmitted to the end-user over a public network such as the Internet. Secure Sockets Layer (SSL) encryption is a proven technology used by the military, banks, online merchants, and Fortune 500 companies to securely transmit confidential information over the Internet. The following measures help ensure communications between the cloud computing provider and the end-user remain confidential:

- Browser-based transmission of sensitive data must use Secure Sockets Layer (SSL)

¹ http://searchcio.techtarget.com/sDefinition/0,,sid182_gci1095696,00.html

² https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

³ <http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html>

Backups and Redundancy

Cloud computing providers are looked to not only provide outsourced hosting of data, but to implement appropriate procedures to ensure all data is backed up and appropriate redundant failovers are in place. The following measures help ensure a cloud computing provider is taking appropriate steps to back up and safeguard their client's data:

- Multiple intra-day backups
- At least one geographically redundant (i.e. stored at a geographically distinct location from primary backups)
- Data center must be served by multiple Internet providers and power grids
- Service Level Agreement specifying minimum guarantee of uptime and remuneration policy if guarantee not met.
- Data center must have at least one week's worth of backup capacity

Confidentiality and Privacy

Cloud computing providers should provide assurances through a Terms of Service or Privacy Policy that all data stored with the provider will be kept confidential, and not used for any purposes other than serving the end user their data:

- Guarantees that no personally identifiable information will be released to third parties unless required by law
- Guarantees that account data will only be accessed with specific authorization of the account-holder to resolve a customer issue
- Privacy policy clearly states all data stored with cloud provider is sole property of the customer
- Include appropriate confidentiality assurances (described further in recommendation #3 "Model Terms of Service for Cloud Computing Providers")

Data Portability

As with all software systems, users of cloud computing providers should be free to export their data for the purposes of migrating to an alternate cloud computing provider, a desktop software product, or to retain separate on-premise backups of data stored with the cloud provider. Storing an on-premise backup of data stored with a cloud computing provider also provides strong protection against scenarios such as the cloud computing provider going out of business or becoming unavailable for any reason:

- All mission-critical, active customer data (at a minimum contact information, matter data, billable time entries, expense entries, and calendar events) will be made available for download, on demand, in a non-proprietary open format such as CSV

Taken as a whole, these security measures represent a level of data protections that all but the largest of firms would find cost-prohibitive to implement, but can be made available to small- and mid-sized firms due to the economies of scale the cloud computing model affords.

The measures above provide a baseline of security and privacy guarantees that allow lawyers to store confidential client data in "the cloud" in good conscience, and in accordance with our understanding of Rule 1.6 of the Rules of Professional Conduct.

3. Model Terms of Service for Cloud Computing Providers

One of the questions suggested for consideration by the Commission is if lawyers have an obligation to negotiate specific terms of service with their cloud computing provider.

Needless to say, having to negotiate a separate set of terms and conditions with each lawyer would be an inefficient use of time and come at a huge economic cost to both cloud computing providers and end-users. Negotiating, approving, tracking, and servicing a customer base that consisted of different baseline service Terms for different customers would be, as a practical matter, virtually impossible. Cloud computing is not special in this regard. The uniform nature of terms in high-transaction volume services is unique to neither cloud computing nor web services in general; rather, such terms are a routine, recurring part of normal "offline" business. (For example, lawyers are not required to negotiate unique, individualized or personalized Terms with their cellular phone provider, internet access provider, overnight delivery service, or physical document storage facility, or traditional desktop software).

That said, given the unique and elevated ethical obligations of attorneys, we do believe that attorneys should verify that Provider Terms contain a clear, concise, "plain English" description of their policies with respect to certain key matters. In addition, Terms should be made reasonably available for review at no charge prior to, during, and after a subscription period.

One solution to explore is the development of a set of standardized Terms that are responsive to the needs and interests of law firms. If a cloud computing vendor or hosting provider is aware of a set of standardized Terms that are legal industry specific and adopts such terms as part of a commitment to "best practices", the process of law firm review and decision-making about the acceptability of a particular cloud computing vendor can be greatly simplified. Such standardization may also have an impact on the willingness of the law firm's malpractice carrier to extend coverage to the online delivery of legal services and other law activities that are conducted in the cloud.

Standardized Terms and Conditions that should be incorporated into agreements between cloud computing vendors and law firms should address the following issues:

(a) Data Ownership. Data uploaded by a law firm to a licensed account (such as contact records, documents, or calendar entries) should remain the property of that law firm. Providers should not claim any ownership rights in such data whatsoever (by express or implied lien, operation of law, or otherwise); provided, however, such data may be subject to rules with respect to accessibility and/or deletion.

(b) Data Accessibility. Policies with respect to accessibility and availability of data both during and after an active subscription period (including the available methods of export or retrieval) should be detailed in the Terms. Terms should disclose what type of data export methods may be available, policies with respect to scheduling retrieval (if applicable) and additional cost associated with retrieval, if any.

(c) Data Backup and Storage. Providers should give a general description of their data backup and storage practices (such as general frequency and timing) and additional costs applicable (if any), but may exercise reasonable discretion as to the level of detail disclosed so as not to impair security.

(d) Security, Confidentiality and Privacy. Providers should disclose their general security practices with respect to matters such as system access (e.g. who has access to data, and under what circumstances) and data encryption, including whether personnel, contractors, and third-party business partners (if applicable) are subject to confidentiality obligations, but may exercise reasonable discretion as to the level of detail disclosed so as not to impair security. In addition, Providers should indicate their compliance with any applicable federal and state laws governing data privacy, and their policy for handling subpoenas or similar official requests to produce, disclose, or otherwise grant third-party access to an account. Providers should also disclose whether they use an offsite hosting company and, if so, whether: (i) servers are located in the United States (servers located outside the United States may be subject to different laws); and (ii) the company abides by security and privacy terms at least as protective as Provider.

4. Is Cloud Computing Outsourcing?

The Commission proposes a new Comment 3 to Rule 5.3, **Responsibilities Regarding Nonlawyer Assistants**, which seeks to make clear that the rule applies not only to the supervision of legal assistants and lawyers, but to any “nonlawyer service providers outside the lawyer’s or law firm’s office.” A literal reading of the language suggests that such non-legal, nonlawyer service providers such as the firm’s accounting firm or bookkeeping firm, FedEx and other courier and delivery companies, web site hosting providers, web-based mail list management companies such as ConstantContact, hosted email providers such as Google, Yahoo, hosted Microsoft Exchange Servers, and SaaS (software-as-a-service) vendors, such as Salesforce.com, Intuit, and SaaS legal application and practice management providers, are all within the definition of “nonlawyer service providers.” However, none of these non-legal, nonlawyer service providers are involved in the direct delivery of legal services, as attorneys and legal assistants are.

While we understand the Commission’s concern that the requirements of Rule 1.6 be complied with, lawyers have always contracted for outside non-legal services, using their professional and management judgment to weigh the risks of contracting which will vary, depending on the circumstances.

We have some concerns that this new Comment #3, will be a cause of confusion among lawyers who are in the process of making decisions on the most cost effective way to purchase non-legal support services. There is a difference between outsourced service providers such as legal assistants and lawyers who are engaged directly in the delivery of legal services, and non-legal, nonlawyer service providers not engaged directly in the delivery of legal services.

Here are our concerns:

First, while it has always been the case that lawyers have been required to use their professional judgment in contracting for these services, the term “reasonable efforts”, as used in Comment #3, is subject to interpretation could be a cause of confusion when a lawyer or a firm decides to enter into a contractual relationship for such non-legal services.

Second, the statement that: “If information protected by Rule 1.6 will be disclosed to nonlawyer service providers outside the lawyer’s or law firm’s office, informed client consent to such disclosure may be required” can cause further confusion without a further explanation of when disclosure may be required and the nature of such disclosures.

In order for a client to give “informed consent”, the attorney must have knowledge of the risks involved in the disclosure and be able to explain to clients the nature of those risks. In particular, we do not believe presently, that most lawyers, particularly solo practitioners and lawyers in small law firms which do not have access to extensive IT experts or resources, have a sufficient understanding of the new web-based technologies that are the underpinning of hosted web services, and the risks associated with the use of those technologies. In order for Comment #3 to have any practical impact, the American Bar Association needs to assume an educational role through publications, white papers, and web-based CLE resources that are designed to provide guidance to the typical practitioner in this area. Our fear, is that without such guidance, lawyers may retreat from adopting web-based technologies and the benefits that these technologies promise, because of fear that they are not in compliance with the requirements of Rule 5.3.

Third, in our opinion, any amendments to the Rules that would require lawyers to directly supervise the work of non-legal service providers would be an impractical burden for the lawyer and likely result in the lawyer or firm avoiding the use of such services, however valuable, to avoid violating the Rules of Professional Responsibility. It makes sense to require the lawyer to have a duty to supervise the work of legal assistants and lawyers who perform work outside of the law firm when they are engaged directly in the delivery of legal services. To require that the lawyer also supervise the work of the kind of non-legal vendor as listed above would be excessive and intrusive in terms of regulating the management practices of a law firm.

5. Cloud Computing Security Vis-à-vis E-mail Security

In assessing the security and privacy of cloud computing, e-mail provides a useful reference point because of its relative maturity as a technology. In 1999, the ABA issued Formal Ethics Opinion No. 99-143 indicating unencrypted e-mail communications provided a “reasonable expectation of privacy” from both a technical and legal standpoint:

“The Committee believes that e-mail communications, including those sent unencrypted over the Internet, pose no greater risk of interception or disclosure than other modes of communication commonly relied upon as having a reasonable expectation of privacy.”

From a security and privacy standpoint, cloud computing technology is in every way superior to unencrypted e-mail. Unlike e-mail, most cloud computing providers encrypt all communications using SSL encryption, and take active measure to secure and control data flows. Using e-mail as a technological baseline that the ABA deems to provide a reasonable expectation of privacy, it is clear to us that cloud computing technology, if assessed by the same criteria, also provides a reasonable expectation of privacy. In this document, recommendation #2 “Minimal Set of Technology Standards for Cloud Computing Providers” provides guidance to law firms looking to understand cloud-computing vendor’s responsibilities regarding encryption, security, and more.

Please accept our sincere thanks for your consideration of the aforementioned recommendations.

We would be pleased to work with the Commission to develop a set of standardized Terms and Conditions that would be incorporated in agreements between cloud computing vendors and law firms as proposed in this letter.

We are available for further comment or clarification at your convenience the via the contact details below.

Sincerely,

The Legal Cloud Computing Association

Jack Newton
President, Clio (Themis Solutions Inc.)

Richard Granat
President, DirectLaw Inc.

Larry Port
Founding Partner and Chief Software Architect, RocketMatter LLC

David Dahl,
CTO, Total Attorneys, LLC