THE IOWA STATE BAR ASSOCIATION

Committee on
Ethics and Practice Guidelines

September 9, 2011

Mr. Dwight Dinkla J.D.
Executive Director
Iowa State Bar Association
625 East Court
Des Moines, IA 50309

RE: Ethics Opinion 11-01 Use of Software as a Service – Cloud Computing

Dear Mr. Dinkla,

The Committee has been asked to address whether a lawyer or law firm may utilize what is known as "software as a service" commonly referred to as "SaaS". The American Bar Association's Legal Technology Resource Center explains SaaS as follows:

SaaS is distinguished from traditional software in several ways. Rather than installing the software to your computer or the firm's server, SaaS is accessed via a web browser (like Internet Explorer or FireFox) over the Internet. Data are stored in the vendor's data center rather than on the firm's computers. Upgrades and updates, both major and minor, are rolled out continuously.... SaaS is usually sold on a subscription model, meaning that users pay a monthly fee rather than purchasing a license up-front.

Because SaaS involves storing client information on computer servers that are not owned and operated by the lawyer or law firm, lawyers have questioned whether SaaS can be used in light of Iowa Rule of Professional Conduct 32:1.6 Comment [17]

317 Sixth Avenue
Des Moines, IA 50309
Phone: 515-243-3122
E-Mail: Nick@CritelliLaw.com

Rule 32:1.6 [Comment 17] states:

> [17] 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. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this rule.

We believe the Rule establishes a reasonable and flexible approach to guide a lawyer's use of ever-changing technology. It recognizes that the degree of protection to be afforded client information varies with the client, matter and information involved. But it places on the lawyer the obligation to perform due diligence to assess the degree of protection that will be needed and to act accordingly.

Access to stored data and data protection should be taken into consideration when performing due diligence. Whatever form of SaaS is used, the lawyer must ensure that there is unfettered access to the data when it is needed. Likewise the lawyer must be able to determine the nature and degree of protection that will be afforded the data while residing elsewhere.

It is beyond the Committee's ability to conduct a detailed information technology analysis regarding accessibility and data protection used by the presently available SaaS services. Even if we had that ability our analysis would soon be outdated. Instead we prefer to give basic guidance regarding the implementation of the standard described in Comment 17.

Accessibility

We suggest that lawyers intending to use SaaS , or other information technology services that store the lawyer's work product and client information on servers that are not owned by the lawyer, should ask the following questions:

1. Access:

Will I have unrestricted access to the stored data? Have I stored the data elsewhere so that if access to my data is denied I can acquire the data via another source?

2. Legal Issues:

Have I performed "due diligence" regarding the company that will be storing my data? Are they a solid company with a good operating record and is their service recommended by others in the field? What country and state are they located and do business in? Does their end user's licensing agreement (EULA) contain legal restrictions regarding their responsibility or liability, choice of law or forum, or limitation on damages? Likewise does their EULA grant them proprietary or user rights over my data?

3. Financial Obligation:

What is the cost of the service, how is it paid and what happens in the event of non-payment? In the event of a financial default will I lose access to the data, does it become the property of the SaaS company or is the data destroyed?

4. Termination:

How do I terminate the relationship with the SaaS company? What type of notice does the EULA require. How do I retrieve my data and does the SaaS company retain copies?

Data Protection

In addition to the concepts covered above, lawyers intending to use SaaS should also perform due diligence regarding the degree of protection that will be afforded the data:

1. Password Protection and Public Access:

Are passwords required to access the program that contains my data? Who has access to the passwords? Will the public have access to my data? If I allow non-clients access to a portion of the data will they have access to other data that I want protected?

2. Data Encryption:

Recognizing that some data will require a higher degree of protection than others, will I have the ability to encrypt certain data using higher level encryption tools of my choosing?

Lawyer's Use of Information Technology Due Diligence Services

The Committee recognizes that performing due diligence regarding information technology can be complex and requires specialized knowledge and skill. This due diligence must be performed by individuals who possess both the requisite technology expertise and as well as an understanding of the Iowa Rules of Professional Conduct. The Committee believes that a lawyer may discharge the duties created by Comment 17 by relying on the due diligence services of independent companies, bar associations or

other similar organizations or through its own qualified employees.

For the Committee,

NICK CRITELLI, Chair
Iowa State Bar Association
Ethics and Practice Guidelines Committee