Proposed 2010 Formal Ethics Opinion 7
Subscribing to Software as a Service While Fulfilling the Duties of Confidentiality and Preservation of Client Property
April 15, 2010

Proposed opinion rules that a law firm may contract with a vendor of software as a service provided the risks that confidential client information may be disclosed or lost are effectively minimized.

Inquiry #1:

Much of software development, including the specialized software used by lawyers for case/practice management, document management and billing/financial management, is moving to the "software as a service" (SaaS) model. In the article "Software as a Service (SaaS) Definition and Solutions," Meridith Levinson, writing for the CIO website, explains SaaS as follows:

> Generally speaking, it's software that's developed and hosted by the SaaS vendor and which the end user customer accesses over the Internet. Unlike traditional packaged applications that users install on their computers or servers, the SaaS vendor owns the software and runs it on computers in its data center. The customer does not own the software but effectively rents it, usually for a monthly fee.[1]

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 is 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. And perhaps most importantly, SaaS is usually sold on a subscription model, meaning that users pay a monthly fee rather than purchasing a license up front.[2]

SaaS for law firms may involve the storage of a law firm's data, including client files, billing information, and work product, on remote servers rather than on the law firm's own computer and, therefore, outside the direct control of the firm's lawyers. Given the duty to safeguard confidential client information, including protecting that information from unauthorized disclosure; the duty to protect client property from destruction, degradation or loss (whether from system failure, natural disaster, or dissolution of a vendor's business); and the continuing need to retrieve client data in a form that is usable outside of the vendor's product[3]; may a law firm use SaaS?

Opinion #1:

Yes, provided steps are taken effectively to minimize the risk of inadvertent or unauthorized disclosure of confidential client information and to protect client property, including file information, from risk of loss.

Rule 1.6 of the Rules of Professional Conduct states that a lawyer may not reveal information relating to the representation of a client unless the client gives informed consent or the disclosure is impliedly authorized to carry out the representation. Comment [17] explains, "A lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision." Comment [18] adds that, when transmitting confidential client information, a lawyer must take "reasonable precautions to prevent the information from coming into the hands of unintended recipients."

Rule 1.15 also requires a lawyer to preserve client property, including information in a client's file such as client documents and lawyer work product, from risk of loss due to destruction, degradation or loss. *See also* RPC 209 (noting the "general fiduciary duty to safeguard the property of a client"); RPC 234 (duty to store original documents with legal significance in a safe place or return to client); and 98 FEO 15 (lawyer must exercise "due care" when selecting depository bank for trust account).

Although a lawyer has a professional obligation to protect confidential information from unauthorized disclosure, the Ethics Committee has long held that this duty does not compel any particular mode of handling confidential information nor does it prohibit the employment of vendors whose services may involve the handling of documents or data containing client information. *See* RPC 133 (no requirement that firm's waste paper be shredded if lawyer ascertains that persons or entities responsible for the disposal employ procedures that effectively minimize the risk that confidential information may be disclosed). Moreover, the committee has held that, while the duty of confidentiality extends to the use of technology to communicate, "this obligation does not require that a lawyer use only infallibly secure methods of communication." RPC 215. Rather, the lawyer must use reasonable care to select a mode of communication that, in light of the circumstances, will best protect confidential communications and the lawyer must advise effected parties if there is reason to believe that the chosen communications technology presents an unreasonable risk to confidentiality. Id.

Furthermore, in 2008 FEO 5, the committee has already held that the use of a web-based document management system that allows both the law firm and the client access to the client's file is permissible:

> provided the lawyer can fulfill his obligation to protect the confidential information of all clients. A lawyer must take steps to minimize the risk that confidential client information will be disclosed to other clients or to third parties. *See* RPC 133 and RPC 215….A security code access procedure that only allows a client to access its own confidential information would be an

> appropriate measure to protect confidential client information….If the law firm will be contracting with a third party to maintain the web-based management system, the law firm must ensure that the third party also employs measures which effectively minimize the risk that confidential information might be lost or disclosed. See RPC 133.

In a recent ethics opinion, the Arizona State Bar's Committee on the Rules of Professional Conduct, concurred with 2008 FEO 5, holding that a law firm may use an online file storage and retrieval system that allows clients to access their files over the Internet provided the firm takes reasonable precautions to protect the security and confidentiality of client documents and information.[4]

In light of the above, the Ethics Committee concludes that a law firm may use SaaS if reasonable care is taken effectively to minimize the risks to the confidentiality and to the security of client information and client files. However, the law firm is not required to guarantee that the system will be invulnerable to unauthorized access.[5] Note that no opinion is expressed on the business question of whether SaaS is suitable for a particular law firm.

Inquiry #2:

Are there any "best practices" that a law firm should follow when contracting with a SaaS vendor to minimize the risk?

Opinion #2:

Yes, a lawyer should be able to answer the list of questions below satisfactorily in order to conclude that the risk has been minimized. However, the list is not all inclusive and consultation with a security professional competent in the area of online computer security is recommended when contracting with a SaaS vendor. Moreover, given the rapidity with which computer technology changes, what may constitute reasonable care may change over time and a law firm would be wise periodically to consult with such a professional.

The lawyer or law firm should be able to answer the following questions sufficiently to conclude that the risk to confidentiality and security of client file information is minimal[6]:

- What is the history of the SaaS vendor? Where does it derive funding? How stable is it financially?
- Has the lawyer read the user or license agreement terms, including the security policy, and does he/she understand the meaning of the terms?
- Does the SaaS vendor's Terms of Service or Service Level Agreement address confidentiality? If not, would the vendor be willing to sign a confidentiality agreement in keeping with the lawyer's professional responsibilities? Would the vendor be willing to include a provision in that agreement stating that the

employees at the vendor's data center are agents of the law firm and have a fiduciary responsibility to protect client information?

- How does the SaaS vendor, or any third party data hosting company, safeguard the physical and electronic security and confidentiality of stored data? Has there been an evaluation of the vendor's security measures including the following: firewalls, encryption techniques, socket security features, and intrusion-detection systems?
- Has the lawyer requested copies of the SaaS vendor's security audits?
- Where is data hosted? Is it in a country with less rigorous protections against unlawful search and seizure?
- Who has access to the data besides the lawyer?
- Who owns the data—the lawyer or SaaS vendor?
- If the lawyer terminates use of the SaaS product, or the service otherwise has a break in continuity, how does the lawyer retrieve the data and what happens to the data hosted by the service provider?
- If the SaaS vendor goes out of business, will the lawyer have access to the data and the software or source code?
- Can the lawyer get data "off" the servers for the lawyer's own offline use/backup? If the lawyer decides to cancel the subscription to SaaS, will the lawyer get the data? Is data supplied in a non-proprietary format that is compatible with other software?
- How often is the user's data backed up? Does the vendor backup data in multiple data centers in different geographic locations to safeguard against natural disaster?
- If clients have access to shared documents, are they aware of the confidentiality risks of showing the information to others? *See* 2008 FEO 5.
- Does the law firm have a back-up for shared document software in case something goes wrong, such as an outside server going down?

---

[1] http://www.cio.com/article/109704/Software_as_a_Service_SaaS_Definition_and_Solutions Meridith Levinson, *Software as a Service (SaaS) Definition and Solutions*, CIO.com (March 15, 2007; accessed March 4, 2010)

[2] *FYI: Software as a Service (Saas) for Lawyers*, ABA Legal Technology Resource Center < http://www.abanet.org/tech/ltrc/fyidocs/saas.html>.

[3] Id.

[4] Arizona State Bar Committee on Rules of Professional Conduct, Opinion 09-04 (Dec. 9, 2009).

[5] Id.

[6] Erik Mazzone, Director of Center for Practice Management, North Carolina Bar Association (in email communications with counsel to the Ethics Committee, 3/30/10 and 3/31/10) and ABA Legal Technology Resource Center, see fn. 2.