OPINION 2010-6

DIGEST:

Vermont attorneys can utilize Software as a Service in connection with confidential client information, property, and communications, including for storage, processing, transmission, and calendaring of such materials, as long as they take reasonable precautions to protect the confidentiality of and to ensure access to these materials.

QUESTIONS PRESENTED

The Vermont Bar Association Professional Responsibility Section has been asked to address the propriety of use by attorneys and law firms of Software as a Service ("SaaS") which is also known as Cloud Computing. Subsidiary questions include whether client documents and information can be remotely stored and backed up using SaaS systems; whether there is any subset of client property that cannot be stored using SaaS; whether lawyers can use SaaS and web-based email and calendaring systems; and whether use of remote document synchronization systems is permissible.

RELEVANT RULES

Rule 1.6. Confidentiality of Information

(a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent . . . .

Comments to Rule 1.6: Acting Competently to Preserve Confidentiality

[16] 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.

[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.

Rule 1.1. Competence

A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

Rule 1.15. Safekeeping Property
(a)(1) A lawyer shall hold property of clients or third persons that is in a lawyer's possession in connection with a representation separate from the lawyer's own property. . . . [Client] property shall be identified as such and appropriately safeguarded.

Rule 5.3. Responsibilities Regarding Nonlawyer Assistants
With respect to a nonlawyer employed or retained by or associated with a lawyer:
(a) a partner, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that the person's conduct is compatible with the professional obligations of the lawyer;
(b) a lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer . . .

DISCUSSION

SaaS and Cloud Computing refer to a constellation of web-based data processing, transmission, and storage services that are available over the internet. In the past, client property was handled and stored on site, and lawyer-client communications occurred in person. Technological advances, however, have changed the way data is transmitted and stored, and the ways lawyers communicate with clients. These changes in technology have been accompanied by new questions about how lawyers should act to protect confidentiality of client information.

The propriety of lawyers using SaaS has attracted significant attention from Bar Association Ethics Committees in recent years, and a consensus position has been developing that allows lawyers to store client data in web based systems, and about the steps lawyers should consider and take when engaging in Cloud Computing. This opinion therefore now turns to a summary of recent ethics decisions addressing SaaS.

North Carolina Proposed Formal Ethics Opinion No. 6

Over a period spanning approximately 1½ years, the North Carolina State Bar Association has issued successive drafts of a formal ethics opinion addressing attorney use of SaaS. The third draft of this Formal Ethics Opinion, issued in October 2011, endorses the use of SaaS to store law firm data, including confidential client information, as long as steps are taken to protect the confidentiality of client information and to preserve client property. Proposed NC FEO 6 steps back from a series of mandatory steps that lawyers would have been required to take in connection with use of SaaS, as set forth in the previous April 2011 draft of this Opinion. Instead, the Opinion now provides that lawyers:

> "may use SaaS if reasonable care is taken to minimize the risks of inadvertent disclosure of confidential information and to protect the security of client information and client files. A lawyer must fulfill the duties to protect client information and to safeguard client files by applying the same diligence and competency to manage the risks of SaaS that the lawyer is required to apply when representing clients."

Because of the rapidly changing nature of technology, Proposed NC FEO 6 declines to impose specific requirements on lawyers who use Cloud Computing in connection with client data. Instead, the Opinion identifies a series of steps that lawyers should consider taking before using SaaS, and requires lawyers to engage in ongoing due diligence and continuing legal education to ensure that remotely stored client data remains secure and accessible. Factors identified in this Opinion for those who use SaaS include:

a. Understanding and protecting against security risks inherent in the internet, including end-user vulnerabilities in the lawyer's office;
b. Including provisions about protection of client confidences in the agreement between the lawyer and the SaaS vendor;
c. Ensuring that there are mechanisms for obtaining access to, retrieving, and protecting data if the lawyer terminates use of the SaaS product, or if the SaaS vendor goes out of business or experiences a break in continuity;
d. Carefully reviewing the terms of the user agreement, including its security provisions;
e. Evaluating the security measures used by the vendor; and
f. Confirming the extent to which the SaaS vendor backs up the data it is storing.

Iowa State Bar Association Ethics & Practice Committee Opinion 11-01

In September 2011, the Iowa State Bar Ethics and Practice Committee took a similar approach to Cloud Computing in Opinion 11-01. Applying comment 17 to Rule 1.6, Opinion 11-01 recognized 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."

The Opinion declines to address in detail the specifics of individual SaaS products, because such guidance would quickly prove outdated, and may be beyond the scope of a lawyer's expertise. Instead, Opinion 11-01 suggests a series of matters into which lawyers should inquire before storing client data on remote servers they do not control, including:

a. Availability of unrestricted access to the data, and ability to access the data through alternate means;
b. Performance of due diligence about the SaaS vendor, including its operating record, recommendations by other users, the provider's operating location, its end user agreement (including provisions on choice of law, limitations on liability and damages, and rights in the stored data);
c. Financial arrangements, including access to data in case of nonpayment or default;
d. Arrangements upon termination of relationship with SaaS provider, including access to data; and
e. Nature of confidentiality protections, including password protection and availability of different levels of encryption.

The Opinion further notes that lawyers may be able to discharge their responsibilities by relying on due diligence efforts by non-lawyer personnel with expertise in these areas.

Pennsylvania Bar Association Formal Opinion 2011-200

In its recent Formal Opinion 2011-200, the Pennsylvania Bar Association Committee on Legal Ethics and Professional Responsibility similarly concluded that attorneys can use cloud computing if stored materials remain confidential, and reasonable steps are taken to protect stored data from risks including security breaches and loss of data. This Pennsylvania Opinion recommends various steps the lawyer should explore with the SaaS vendor, including:

a. the existence of an obligation imposed on the vendor to preserve security;
b. a mechanism for the vendor to notify the lawyer if a third party requests access to the stored information;
c. the existence of systems that are sufficient to protect the data from unauthorized access;
d. an agreement about how confidential client information will be protected;
e. the ability to review the vendor's security systems; and
f. tools to protect the lawyer's ability to access and retrieve the data.

California Bar Professional Responsibility and Conduct Committee Formal Op. 2010-179

Recognizing that a technology-specific opinion "would likely become obsolete shortly," California Bar Ethics Opinion 2010-179 similarly endorses Cloud Computing, and then provides a general analysis of the considerations a lawyer should evaluate when using SaaS, including:

a. The ability of the lawyer to assess the security provided by the provider, including the specifics of the technology, whether specific precautions can be used to increase the level of security, and limits on who is permitted to monitor use of the software, evaluated by someone who possesses a sufficient level of competence to address these issues;
b. Availability of legal consequences for improper interception of or access to the data;
c. Degree of sensitivity of the information being stored
d. Potential impact of unauthorized disclosure on the client;
e. Urgency of the situation; and
f. Client circumstances and instructions.

New York State Bar Professional Ethics Committee Opinion 842

In September 2010, the New York State Bar Professional Ethics Committee issued a similar opinion, adopting a reasonableness standard and discussing the following factors that a lawyer should consider when storing client information in the cloud:

a. Confirming that the SaaS vendor has a enforceable duty to maintain security and confidentiality, including prompt notification of the attorney upon service of process requiring disclosure of the data;
b. Investigating the provider's security procedures, policies, and methods for recovering data;
c. Guarding against infiltration attempts using available technology;
d. Determining whether the vendor can transfer and then permanently delete the data if the lawyer changes providers;
e. Periodically reconfirming that security and access measures remain sufficient as technologies change; and
f. Remaining current on the law with respect to changing technologies to ensure that client data is not subject to legal risk, including waiver of confidentiality.

Other Opinions and Authorities

Ethics opinions issued by other State Bar Associations have taken similar positions.

State Bar of Arizona Ethics Opinion 09-04, for example, reaffirms the conclusion drawn in its prior Ethics Opinion 05-04, and concludes that attorneys can use online storage and retrieval systems for client documents and information as long as they take reasonable precautions to ensure that the materials are safe and confidential. This Arizona Opinion further notes that lawyers should recognize that their expertise with respect to technology may be limited and should therefore ensure review of precautions by competent personnel, and periodically review systems to ensure that security precautions remain reasonable.

Opinion 701 of the New Jersey Advisory Committee on Professional Ethics discusses the benefits that may arise from web-based digital storage of and access to client documents and information, and then provides as follows:

> "The critical requirement . . . is that the attorney 'exercise reasonable care' against the possibility of unauthorized access to client information. A lawyer is required to exercise sound professional judgment on the steps necessary to secure client confidences against foreseeable attempts at unauthorized access. 'Reasonable care,' however, does not mean that the lawyer absolutely and strictly guarantees that the information will be utterly invulnerable against all unauthorized access. Such a guarantee is impossible, and a lawyer can no more guarantee against unauthorized access to electronic information than he can guarantee that a burglar will not break into his file rom, or that someone will not illegally intercept his mail or steal a fax."

Opinion 701 continues by noting that the content of the obligation to exercise reasonable care depends on the circumstances and must be informed by the available technology, and personnel handling client information must be subject to an enforceable obligation to preserve confidentiality and security. In addition, Opinion 701 excludes original "client property" from its holding, and notes that lawyers must continue to maintain certain original documents, like wills, trusts, deeds, contracts, and corporate bylaws and minutes, and cannot rely solely on digital storage of these materials. This Opinion further stresses the importance of client consent with respect to remote storage of client information.

To similar effect are Ethics Opinion 2010-02 issued by the Alabama State Bar Association, and Formal Opinion No. 33 issued by the State Bar of Nevada Standing Committee on Ethics and Professional Responsibility. Many other resources also are available about the use of SaaS, including the ABA Commission on Ethics 20/20 Working Group's September 20, 2010 white papers discussing SaaS, and the Law Society of British Columbia's July 15, 2011 Report of the Cloud Computing Working Group.

CONCLUSION

The Vermont Bar Association Professional Responsibility Section agrees with the consensus view that has emerged with respect to use of SaaS. Vermont lawyers' obligations in this area include providing competent representation, maintaining confidentiality of client information, and protecting client property in their possession. As new technologies emerge, the meaning of "competent representation" may change, and lawyers may be called upon to employ new tools to represent their clients. Given the potential for technology to grow and change rapidly, this Opinion concurs with the views expressed in other States, that establishment of specific conditions precedent to using SaaS would not be prudent. Rather, Vermont lawyers must exercise due diligence when using new technologies, including Cloud Computing. While it is not appropriate to establish a checklist of factors a lawyer must examine, the examples given above are illustrative of factors that may be important in a given situation. Complying with the required level of due diligence will often involve a reasonable understanding of:

a. the vendor's security system;
b. what practical and foreseeable limits, if any, may exist to the lawyer's ability to ensure access to, protection of, and retrieval of the data;
c. the material terms of the user agreement;
d. the vendor's commitment to protecting confidentially of the data;
e. the nature and sensitivity of the stored information;
f. notice provisions if a third party seeks or gains (whether inadvertently or otherwise) access to the data; and
g. other regulatory, compliance, and document retention obligations that may apply based upon the nature of the stored data and the lawyer's practice.

In addition, the lawyer should consider:

a. giving notice to the client about the proposed method for storing client data;
b. having the vendor's security and access systems reviewed by competent technical personnel;
c. establishing a system for periodic review of the vendor's system to be sure the system remains current with evolving technology and legal requirements; and
d. taking reasonable measures to stay apprised of current developments regarding SaaS systems and the benefits and risks they present.

In summary, and with respect to the specific questions posed, the Professional Responsibility Section responds as follows.

Vermont attorneys may use SaaS systems for storing, processing, and retrieving client property, as long as they take reasonable precautions to ensure the property is secure and accessible. The nature of the precautions depends on the circumstances. The ability to engage in Cloud Computing is not limited by the specific location of the remote server, although some of the factors noted above, including choice of law clauses, and concerns about access to data in the event of a service interruption or an emergency, may be implicated by the location of the storage server and the extent of backup service provided by the vendor.

Depending on the circumstances, there may be limits on systems that can be used and client property that can be stored with an SaaS vendor, and lawyers must assess each situation

based upon the specific facts and circumstances. For example, it may not be appropriate to rely solely on remote digital storage for preservation of original client property like wills, or other client documents that are subject to permanent retention obligations. Similarly, given that Cloud Computing involves storage of information in the hands of a third party, a lawyer handling particularly sensitive client property, like trade secrets may conclude after consultation with the client that remote SaaS storage is not sufficiently secure.

A lawyer's use of email, calendar, and remote synchronization systems, including systems that are web-based and offered by SaaS vendors, is subject to the same inquiry. Before using such systems, the lawyer should take reasonable precautions to ensure that information in the system is secure and accessible.

Finally, given the rapidly changing nature of technology and the significant manner in which new technologies impact the legal practice including the manner in which confidential client information is communicated and stored, the Professional Responsibility Section invites the Vermont Supreme Court to examine whether changes in applicable Rules of Procedure and Rules of Professional Conduct are warranted to address these issues.