NEBRASKA ETHICS ADVISORY OPINION FOR LAWYERS

NO. 19-01

I. Questions Presented

May an attorney transmit information relating to the representation of a client over the internet and allow for that information to be stored on, and accessed through, third-party, off-site servers (generically referred to as "the Cloud")?

II. Summary of Opinion

An attorney may transmit information relating to the representation of a client over the internet and allow for that information to be stored on, and accessed through, third-party, off-site servers (generically referred to as "the Cloud"), if the lawyer has undertaken reasonable efforts to: (1) prevent inadvertent or unauthorized access to that information; (2) maintain the confidentiality of the information; and (3) establish reasonable safeguards to ensure the information is protected from loss, breaches, business interruptions, and other risks created by advancements in technology.

III. Statement of Facts

Advances in various areas of technology – in storing client data, delivering legal services, simultaneously retrieving stored client data from multiple electronic devices, and communicating the legal advice generated from this client data – have changed the way the legal community stores, accesses, retrieves, and disseminates client information. To address these technological advancements, lawyers and law firms must rely on specialized software developed specifically for the legal industry, possibly even individualized for the lawyer or law firm. This software is utilized for case or practice management, time and billing, document assembly and dissemination, and trial preparation and presentation.

Many lawyers and law firms utilizing this specialized legal software follow the traditional software model: lawyers purchase the software by license (individually or in bulk) and install it onto their (or their paralegal's or assistant's) computers via disk or download. Data created and used by the software (often in a proprietary environment) is stored on the user's computer and often backed up to the firm's central file server. Software updates and security patches are applied occasionally, but for the most part, the software's functionality remains static. Every few years the software developer will release a major revision to the software which requires a new license.

In recent years, a new software model has emerged: Software as a Services (or "SaaS"). SaaS, delivered by a third-party services provider, is accessed via a web browser (like Internet Explorer, Google Chrome, or Mozilla Firefox) over the internet, rather than being installed to the lawyer's computer of the firm's server. Client-specific legal information is stored in the service provider's data center rather than on the firm's computers. This third-party data center is commonly referred to as the Cloud and the use of SaaS to access information from the Cloud is commonly referred to as Cloud Computing.

Upgrades and updates to the software, both major and minor, that allow for a lawyer or law firm to access the Cloud in a variety of diverse ways at almost any hour of the day, are rolled out continuously, allowing the SaaS to be constantly refined and/or personalized. SaaS can include long-term storage and accessibility of confidential client matters or short-term storage that enables specific data processing needs. SaaS is usually sold on a subscription model, requiring end-users to pay a monthly fee in exchange for the SaaS provider assuming responsibility for the security of the confidential, client-specific legal information. To maintain its viability, the SaaS provider incorporates new, more innovative technologies into the SaaS, providing updates to the software that allow the end-users to access their SaaS through a multitude of devices, with almost every new technological advancement.

IV. Applicable Rules of Professional Conduct

A. § 3-501.6. Confidentiality of information.

(a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).

(b) A lawyer may reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary:

(1) to prevent the client from committing a crime or to prevent reasonably certain death or substantial bodily harm;

(2) to secure legal advice about the lawyer's compliance with these Rules;

(3) to establish a claim or defense on behalf of the lawyer in a controversy between the lawyer and the client, to establish a defense to a criminal charge or civil claim against the lawyer based upon conduct in which the client was involved or to respond to allegations in any proceeding concerning the lawyer's representation of the client; or

(4) to comply with other law or a court order.

(c) The relationship between a member of the Nebraska State Bar Association Committee on the Nebraska Lawyers Assistance Program or an employee of the Nebraska Lawyers Assistance Program and a lawyer who seeks or receives assistance through that committee or that program shall be the same as that of lawyer and client for the purposes of the application of Rule 1.6.

B. § 3-501.1. Competence.

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

Comment [6] To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.

§ 3-501.1 Comment 6 amended June 28, 2017.

V. Discussion

At the intersection of a lawyer's confidentiality obligation and competence obligation to "keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology," is a lawyer's obligation to undertake reasonable efforts to protect client information when using technology.

Neb. Ct. R. of Prof. Cond. § 3-501.1 requires a lawyer to provide competent representation to a client. Comment [6] of Neb. Ct. R. of Prof. Cond. § 3-501.1, amended on June 28, 2017, advises lawyers that to maintain the requisite knowledge and skill for competent representation, a lawyer should keep abreast of the benefits and risks associated with relevant technology. Neb. Ct. R. of Prof. Cond. § 3-501.6 requires a lawyer to not reveal information relating to the representation of a client.

The number of lawyers using the Cloud has attracted significant attention from Bar Association Ethics Committees across the country in recent years, and a consensus position has developed that permits lawyers to store client information in the Cloud if the lawyer undertakes reasonable efforts to protect the information when using the Cloud. This opinion now turns to a summary of recent ethics decisions from across the country addressing SaaS.

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

In September 2011, the Iowa State Bar Ethics and Practice Committee addressed Cloud Computing in Opinion 11-01. The Opinion 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 declined to address in detail the specifics of individual SaaS products, because such guidance would quickly prove outdated. Instead, the Opinion suggested a series of matters into which lawyers should inquire before storing client data on remote servers they do not control, including: (1) availability of unrestricted access to the data, and the ability to access the data through alternate means; (2) 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; (3) financial agreements, including access to date in case of nonpayment or default; (4) arrangements upon termination of relationship with SaaS provider, including access to data; and (5) nature of confidentiality protections, including password protection and availability of different levels of encryption.

B. Pennsylvania Bar Association Committee on Legal Ethics and Professional Responsibility 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. The Opinion recommends various steps which lawyers should explore with the SaaS vendor, including: (1) the existence of an obligation imposed on the vendor to preserve security; (2) a mechanism for the vendor to notify the lawyer if a third party requests access to the stored information; (3) the existence of systems that are sufficient to protect the data from unauthorized access; (4) an agreement about how confidential client information will be protected; (5) the ability to review the vendor's security systems; and (6) tools to protect he lawyer's ability to access and retrieve data.

C. North Carolina 2011 Formal Ethics Opinion 6

North Carolina similarly concluded 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."

The Opinion declined to impose specific requirements on lawyers who use Cloud Computing, but identified the following factors for lawyers to take into account, including: (1) understanding and protecting against security risks inherent in the internet; (2) including provisions about protection of client confidences in the agreement between the lawyer and the SaaS vendor; (3) 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; (4) carefully reviewing the terms of the user agreement, including its security

provisions; (5) evaluating the security measures used by the vendor; and (6) confirming the extent to which the SaaS vendor backs up the data it is storing.

VI. Conclusion

The Nebraska State Bar Association Ethics Advisory Committee agrees with the consensus view that has emerged with respect to the use of the Cloud. As new technologies emerge, the meaning of competence may change, and lawyers will be called upon to employ new technological tools to competently represent their clients. Given that technology grows and changes rapidly, this Opinion follows the views of other states and declines to adopt specific requirements before an attorney uses the Cloud. Instead, lawyers must undertake reasonable efforts to: (1) prevent inadvertent or unauthorized access to that information; (2) maintain the confidentiality of the information; and (3) establish reasonable safeguards to ensure the information is protected from loss, breaches, business interruptions, and other risks created by advancements in technology.