THE PROFESSIONAL ETHICS COMMITTEE
FOR THE STATE BAR OF TEXAS
OPINION NO. 680

September 2018

QUESTION PRESENTED

Under the Texas Disciplinary Rules of Professional Conduct may a lawyer use cloud-based client data storage systems or use cloud-based software systems for the creation of client-specific documents where confidential client information is stored or submitted to a cloud-based system?

STATEMENT OF FACTS

A lawyer is considering subscribing to various cloud-based electronic storage and software systems that allow users to store confidential client information or prepare form legal documents by uploading confidential client information for insertion into those form documents. The lawyer is concerned because these cloud-based electronic storage and software systems are owned by private companies, the various computer servers on which this client confidential information would reside are or may be located in other countries, the client information could be accessed by employees of these private companies, and there is the possibility of these servers and the confidential information residing on them being "hacked" by third parties or being rendered inaccessible as a result of a cloud storage vendor going out of business. The lawyer questions whether it is ethical to use cloud-based electronic storage or software systems given these conditions and the potential disclosure risks to confidential client information.

DISCUSSION

Rule 1.05(a) of the Texas Disciplinary Rules of Professional Conduct broadly defines client "confidential information" as including both "privileged information" and "unprivileged client information." The latter means "all information relating to a client or furnished by the client, other than privileged information, acquired by the lawyer during the course of or by reason of the representation of the client." Rule 1.05(a).

Rule 1.05(b) provides in part that, "[e]xcept as permitted by paragraphs (c) and (d), or as required by paragraphs (e) and (f), a lawyer shall not knowingly:

(1) Reveal confidential information of a client or former client to:

(i) a person that the client has instructed is not to receive the information; or

> (ii) anyone else, other than the client, the client's representatives, or the members, associates, or employees of the lawyer's law firm."

A lawyer violates Rule 1.05 if the lawyer knowingly reveals confidential information to any person other than those persons who are permitted or required to receive the information under paragraphs (b), (c), (d), (e), or (f) of the Rule. The Terminology section of the Rules states that "'[k]nowingly' . . . denotes actual knowledge of the fact in question" and that a "person's knowledge may be inferred from circumstances."

Professional Ethics Opinion 648 (April 2015) addressed the question of whether a lawyer could ethically transmit client confidential information by email. The Committee concluded that, "considering the present state of technology and email usage, a lawyer may generally communicate confidential information by email. Some circumstances, may, however, cause a lawyer to have a duty to advise a client regarding risks incident to the sending or receiving of emails arising from those circumstances and to consider whether it is prudent to use encrypted email or another form of communication." Similarly, Opinion 572 (June 2006) determined that, "[u]nder the Texas Disciplinary Rules of Professional Conduct, unless the client has instructed otherwise, a lawyer may deliver materials containing privileged information to an independent contractor, such as a copy service, hired by the lawyer in the furtherance of the lawyer's representation of the client if the lawyer reasonably expects that the confidential character of the information will be respected by the independent contractor."

Cloud-based electronic storage and software systems are in wide use among the general public and lawyers. While wide usage of an information storage method or software document creation system is not, in itself, justification for its use by lawyers, alternative methods of information storage and document preparation also have an inherent risk of disclosure or misuse—just as a privileged letter to a client through the U.S. Postal Service (versus transmission through email) can be intercepted or accessed by third parties and a client's file in a lawyer's office may be susceptible to access or disclosure by unauthorized parties without the lawyer "knowingly" revealing that information.

Considering the present state of technology, its common usage to store confidential information, and the potential cost and time savings for clients, a lawyer may use cloud-based electronic data systems and document preparation software for client confidential information; however, lawyers should remain continually alert to the vulnerability of cloud-based vendors and systems to data breaches and whether a particular vendor or system appears to be unusually vulnerable, based on systemic failures by that vendor or system of which the lawyer should be aware. In certain circumstances, a lawyer may decide that some client confidential information is too vulnerable to unauthorized access or disclosure to risk its storage or use in a cloud-based electronic system or too vulnerable to such risk without that data being adequately encrypted or without additional technological safeguards in place. Data "hacking" by third parties is becoming increasingly well-known and can even occur with respect to client confidential information

stored on a server within a law firm. Therefore, a lawyer should remain reasonably aware of changes in technology and the associated risks—without unnecessarily retreating from the use of new technology that may save significant time and money for clients. In some circumstances it may be appropriate to confer with a client regarding these risks as applicable to a particular matter and obtain a client's input regarding or consent to using cloud-based electronic data systems and document preparation software. Of course, if a client has given specific instructions regarding the use and protection of its client confidential information in a matter those instructions must be followed except when otherwise required or permitted by the provisions of Rule 1.05.

Still, a lawyer must take reasonable precautions in the adoption and use of cloud-based technology for client document and data storage or the creation of client-specific documents that require client confidential information. These reasonable precautions include: (1) acquiring a general understanding of how the cloud technology works; (2) reviewing the "terms of service" to which the lawyer submits when using a specific cloud-based provider just as the lawyer should do when choosing and supervising other types of service providers; (3) learning what protections already exist within the technology for data security; (4) determining whether additional steps, including but not limited to the encryption of client confidential information, should be taken before submitting that client information to a cloud-based system; (5) remaining alert as to whether a particular cloud-based provider is known to be deficient in its data security measures or is or has been unusually vulnerable to "hacking" of stored information; and (6) training for lawyers and staff regarding appropriate protections and considerations. These precautions do not require lawyers to become experts in technology; however, they do require lawyers to become and remain vigilant about data security issues from the outset of using a particular technology in connection with client confidential information. The Committee refrains from setting out specific requirements for assessing reasonableness since some precautions become obsolete over time with changing technologies and the risks may change as well.

Rule 1.01(a) requires that lawyers exhibit "competence" in representing clients. In Opinion 665 (December 2016), the Committee applied Rule 1.01 to a question involving a lawyer's inadvertent transmission to third parties of electronic metadata within client documents and concluded that the Rule's "competency" requirement was applicable to a lawyer's technological competence in preserving client confidential information. The Committee reiterates here the necessity of competence by lawyers and their staff regarding data protection considerations of cloud-based systems.

CONCLUSION

Under the Texas Disciplinary Rules of Professional Conduct, a lawyer may use a cloud-based electronic data storage system or cloud-based software document preparation system to store client confidential information or prepare legal documents. However, lawyers must remain alert to the possibility of data breaches, unauthorized access, or disclosure of client confidential information and undertake reasonable precautions in using those cloud-based systems.