ETHICS OPINION NO. 263
OF THE MISSISSIPPI BAR
RENDERED June 11, 2020

The Ethics Committee of the Mississippi Bar has been asked to respond to the following question:

Is the use of online cloud-based storage companies (Dropbox, Google Cloud, etc.) a violation of Rule 1.6 of the Mississippi Rules of Professional Conduct?

Analysis

Rule 1.6 of the Rules of Professional Conduct provides in relevant part:

> Rule 1.6. Confidentiality of Information
>
> - 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).

In addition, MRPC 1.1 requires a lawyer to "provide competent representation to a client" and explains that "[c]ompetent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."

MRPC 1.15 addresses a lawyer's duty to safeguard client property, and it requires lawyers to "hold the property of others with the care required of a professional fiduciary." MRPC 1.15, cmt. "The loss of client files constitutes a violation of Rule 1.15." Mississippi Bar v. Thompson, 5 So. 3d 330, 335 (Miss. 2008).

Cloud-based storage involves saving data and software on servers owned by third parties. It is generally accepted that such storage offers many benefits, including the potential for being cheaper and more convenient than traditional physical storage methods. Cloud-based storage may minimize the risk of data loss caused by fires, tornados, hurricanes, earthquakes and other catastrophic physical events. On the other hand, cloud-based storage exposes data to new cybersecurity risks and other risks associated with relinquishing control over data to third parties. Therefore, lawyers must weigh the benefits of cloud-based storage against the new risks presented by that technology. At all times, the paramount consideration should be the protection of client data.

The Committee is of the opinion that lawyers may use a cloud-based electronic data storage system to store client confidential information, but lawyers must undertake reasonable precautions in using those cloud-based systems.

It appears that every state bar association that has addressed this issue (more than 20) has approved it subject to the requirement that lawyers use reasonable care in their implementation of cloud-based storage and their selection of a cloud storage provider. One recent example is the State Bar of Texas. In September 2018, the Professional Ethics Committee for the State Bar of Texas (the "Texas Ethics Committee") issued Opinion No. 680, in which it concluded that, under the Texas Disciplinary Rules of Professional Conduct, a lawyer may use a cloud-based client data storage system to store client confidential information, provided that lawyers 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. The opinion noted that cloud-based storage is in wide use among the general public and lawyers, and alternative storage methods carry their own inherent risks of disclosure or misuse (such as inadvertent disclosure or access to client files in a lawyer's office).

Despite the benefits and relative security of cloud-based storage, the Texas Ethics Committee concluded that lawyers must always be alert to the vulnerability of such systems and take "reasonable precautions" in the adoption and use of cloud-based technology for client data storage. These "reasonable precautions" include:

- acquiring a general understanding of how the cloud technology works;
- 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;
- learning what protections already exist within the technology for data security;
- 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;
- 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
- training for lawyers and staff regarding appropriate protections and considerations.

See also, Illinois State Bar Association Professional Conduct Advisory Opinion No. 16-06 (October 2016) (approving of the use of cloud-based services for the provision of legal services subject to adoption of reasonable measures to protect client information and outlining seven non-exhaustive reasonable inquiries and practices for

the selection of a cloud-based storage service provider); Alabama Ethics Opinion 2010-2 (2010) (lawyer may outsource storage of client files through cloud computing if the lawyer takes reasonable steps to make sure data is protected); Iowa Ethics Opinion 11-01 (2011) (lawyer should conduct appropriate due diligence before storing files electronically); Tennessee Formal Ethics Opinion 2015-F-159 (2015) (a lawyer may allow client information to be stored in the cloud provided the lawyer takes reasonable care to assure that the information remains confidential and that reasonable safeguards are employed to protect the information from breaches, loss or other risks).

The Committee has previously concluded that MRPC 1.6 includes a duty of technological competence with respect to protecting client confidentiality. In Opinion No. 259 (November 29, 2012), the Mississippi Ethics Committee applied Rule 1.6 to a question involving a lawyer's duties with respect to electronic metadata within client documents and concluded that "an attorney has an affirmative duty to take reasonable precautions to ensure that confidential metadata is not inadvertently revealed by an electronic document." In reaching this conclusion, the Committee reasoned that "[n]o new duty for lawyers to protect client confidentiality is created by this Opinion. However, due to the technological advances, a new category of confidential information which is subject to Rule 1.6, MRPC, exists." The Committee also noted that 17 states had reached a similar conclusion, and "[e]very state which has rendered a formal ethics opinion on this issue has concluded that lawyers have an obligation to understand the technology that they utilize and a lawyer sending files in an electronic format must exercise reasonable care in transmitting files in electronic format so as not to disclose client confidences." The Committee similarly concludes here that MRPC 1.6 imposes upon lawyers an affirmative duty to take reasonable precautions to ensure that confidential client data stored in the cloud is not revealed except in the circumstances permitted by Rule 1.6. See also, MRPC 1.1 and 1.15.[1]

The Committee agrees that the inquiries and practices set forth by the Texas Ethics Committee constitute a non-exhaustive list of reasonable inquires, practices and precautions for the selection of cloud-based storage service providers and the adoption of cloud-based storage for client data.

Conclusion

The Committee is of the opinion that lawyers may use a cloud-based electronic data storage system to store client confidential information, but lawyers must undertake reasonable precautions in using those cloud-based systems.

[1] In 2012, the ABA amended Comment 8 to ABA Model Rule 1.1 of the Model Rules of Professional Conduct to make it clear that to comply with the duty of competence, "a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology." (emphasis added). While this particular comment has not yet been adopted by the Mississippi Supreme Court, the Committee is of the opinion that the duty of technological competence is necessarily encompassed in MRPC 1.1.