STATE BAR OF NEVADA

STATE BAR OF NEVADA
STANDING COMMITTEE ON
ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion No. 33
February 9, 2006

BACKGROUND

A Nevada attorney has requested an opinion concerning the application of Supreme Court Rules to the attorney's use of an outside agency to store electronically formatted client information. In the situation posed, the attorney's electronic client files, which contain confidential client information and communications, are stored on a server or other computer device which is physically located and maintained by a third party outside the attorney's direct control and supervision. It is assumed that the attorney can, as part of his or her service contract with the third party, require that all reasonably necessary means be employed by the third party to preserve the confidentiality of the information and to prevent unauthorized access to it and disclosure of it. It is also assumed, however, that employees of the third party agency will, by virtue of their employment, have access, both authorized and unauthorized, to the confidential client information.

QUESTION PRESENTED

The committee has revised the question originally presented to more broadly address the lawyer's duty of confidentiality with respect to electronic client information. The question addressed in this opinion is whether a lawyer violates SCR 156 by storing confidential client information and/or communications, without client consent, in an electronic format on a server or other device that is not exclusively in the lawyer's control.

ANSWER

The lawyer's duty to protect client confidentiality under Supreme Court Rule 156 is not absolute. In order to comply with the rule, the lawyer must act competently and reasonably to safeguard confidential client information and communications from inadvertent and unauthorized disclosure. This may be accomplished while storing client information electronically with a third party to the same extent and subject to the same standards as with storing confidential paper files in a third party warehouse. If the lawyer acts competently and reasonably to ensure the confidentiality of the information, then he or she does not violate SCR 156 simply by contracting with a third party to store the information, even if an unauthorized or inadvertent disclosure should occur.

SUPREME COURT RULE INTERPRETED

Supreme Court Rule 156

AUTHORITIES AND REFERENCES

ABA Committee on Ethics and Professional Responsibility, Formal Opinion No. 99-413 (1999).
ABA Committee on Ethics and Professional Responsibility, Formal Opinion No. 95-398 (1995).
ABA Committee on Lawyers' Responsibility for Client Protection, Lawyers on Line: Ethical

Perspectives in the Use of Telecomputer Communication (1986).
ABA Committee on Professional Ethics, Informal Opinion No. 1127 (1970).
Anderson, J.C., Transmitting Legal Documents over the Internet: How to Protect Your Cient and Yourself, 27 Rutgers Computer & Tech. L.J. 1 (2001).
Annotated Model Rules of Professional Conduct, 5th ed. (ABA, 2003), Rule 1.6 and accompanying commentary.
California Standing Committee on Professional Responsibility and Conduct, Formal Opinion number 1971-25.
Hopkins, R.S. & Reynolds, P.R., Redefining Privacy and Security in the Electronic Communication Age: A Lawyer's Ethical Duty in the Virtual World of the Internet, 16 Geo. J. Legal Ethics 675 (2003).
Winick, M.L., Burris, B. & Bush, Y.D. Playing I Spy with Client Confidences: Confidentiality, Privilege and Electronic Communications, 31 Tex. Tech L. Rev. 1225 (2000).

DISCUSSION

A lawyer must act competently to safeguard against inadvertent or unauthorized disclosure of confidential client information. While a lawyer is not strictly liable for any breach of client confidentiality, his duty includes reasonable precautions to prevent both accidental and unauthorized disclosure. SCR 156; Model Rule 1.6, comment 16. A client, however, may give informed consent to a means of protection that might otherwise be considered insufficient. For purposes of this opinion, however, it is presumed that the client has not waived any right to confidentiality or consented to a means of protection that would otherwise violate the Supreme Court Rules absent informed consent.

Opinions directly addressing this issue, particularly with respect to electronic data, are scarce and somewhat outdated given the recent advances in electronic communications and data processing. Available opinions and commentary added to Model Rule 1.6 by the ETHICS 2000 amendments, however, clearly support the answer stated in this opinion.

The ABA Committee on Professional Ethics, in Informal Opinion No. 1127 (1970) (interpreting former Canon 37), addressed the question whether confidential client information could be stored in a central computer facility, in which the information would be accessible to, but would not necessarily be accessed by, employees of the facility. The committee determined that so long as arrangements were made so that the information transmitted to the data processor was kept in confidence, and the employees of the law firm and the data processor did not permit disclosure to any unauthorized person, then there was no violation of the lawyer's duty of confidentiality. The required "arrangements", in the committee's opinion, consisted of competence and reasonable care in 1) the selection of the third party contractor and 2) an express contractual requirement that the contractor and its employees keep the information confidential and protected from unauthorized access or disclosure.

In Formal Opinion number 1971-25, the California Standing Committee on Professional Responsibility and Conduct responded differently, but to a somewhat different question. That opinion addressed an attorney's transmission of confidential client information, without prior client consent, to a "data processing center for bookkeeping, billing, accounting, and statistical purposes." *Id*. at p. 2. The question there was somewhat different than that presented here in that it was presumed that at least one of the purposes of the transmission of the information to the "data processing center" would necessitate the disclosure of confidential client information to a person or persons not employed, supervised or controlled by the attorney. The committee concluded that without the client's consent, the disclosure of confidential information to a third person in such circumstances violates the attorney's duty of confidentiality.

The issue presented here is more similar to that involved in the ABA committee opinion. The use of an outside data storage or server does not necessarily require the revelation of the data to anyone outside the attorney's employ. The risk, from an ethical consideration,

is that a rogue employee of the third party agency, or a "hacker" who gains access through the third party's server or network, will access and perhaps disclose the information without authorization. In terms of the client's confidence, this is no different in kind or quality than the risk that a rogue employee of the attorney, or for that matter a burglar, will gain unauthorized access to his confidential paper files. The question in either case is whether the attorney acted reasonable and competently to protect the confidential information. The California opinion is thus distinguished by the presumption underlying that opinion that the attorney could exercise no control whatsoever over the confidential information in the hands of the third party contractor.

Subsequent ABA opinions concerning client confidentiality in the electronic age have to some degree reflected the evolution of electronic technology itself. In 1986, an ABA committee issued a report cautioning lawyers against electronic client communications and concluded that an attorney should not communicate with clients electronically without first obtaining the client's informed consent or being reasonably assured of the security of the electronic system in question. ABA Committee on Lawyers' Responsibility for Client Protection, Lawyers on Line: Ethical Perspectives in the Use of Telecomputer Communication (1986). The committee did not ban all such communication, but rather described the lawyer's obligation in this regard as an affirmative duty to competently investigate the electronic communications system and form a reasonably conclusion as to its security. Id.

The ABA Committee addressed an issue much closer to that discussed here in Formal Opinion number 95-398, and concluded that a lawyer may give a computer maintenance company access to confidential information in client files, but that in order to comply with the obligation of client confidentiality, he or she "must make reasonable efforts to ensure that the company has in place, or will establish, reasonable procedures to protect the confidentiality of client information." The ABA Committee recognized in that opinion the growing practicality and availability of third party electronic data services, but clearly concluded that the duty of confidentiality is not breached so long the attorney is reasonable and competent in the creation and management of the outside contractor arrangement.

In a later formal opinion, the ABA Committee continued this trend and retreated substantially from the 1986 opinion concerning the encryption of e-mail. That opinion concluded that sending confidential client communications by unencrypted email does not violate the lawyer's duty of confidentiality because unencrypted email still affords a reasonable expectation of privacy from both legal and technological standpoints. ABA Committee on Ethics and Professional Responsibility, Formal Opinion No. 99-413 (1999). The committee left open the likelihood, however, that cases of particularly sensitive client communications may require extraordinary security precautions, since the reasonableness and competence of the lawyer's actions must be judged in the context of the relative sensitivity of the particular confidential information or communication at stake. See Model Rule 1.6, comments 16 and 17.

Nearly all state bar associations and committees addressing the issue have adopted the ABA's 1999 approach to email communications. Hopkins & Reynolds at 677-78; Winich, Burris & Bush at 1252-1254. Commentators have argued that further advances in technology will increase the lawyer's obligation with respect to electronic client communications and information and that "reasonable" action to protect client confidentiality already may include encryption, virus protection and other similar security measures as they become more efficient and cost effective, and as electronic communications and data storage may eventually be found to afford less than a reasonable expectation of privacy. Hopkins & Reynolds at 691.

The ABA, at least for now, has continued the course set in the 1999 formal opinion, adding two new comments to Model Rule 1.6 to reinforce the view that electronic communications and information require no special security or confidentiality measures that would not otherwise be required in communication in a more traditional format. The new comments

are:

[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.

The previous ABA opinions and the new comments to Rule 1.6 clearly evidence the ABA's policy to treat electronic client communications and information according to existing rules and not to hold an attorney responsible for a breach of client confidentiality, or for storing client information in such a manner that the breach is possible, so long as the attorney:

1. Exercises reasonable care in the selection of the third party contractor, such that the contractor can be reasonably relied upon to keep the information confidential; and

2. Has a reasonable expectation that the information will be kept confidential; and

3. Instructs and requires the third party contractor to keep the information confidential and inaccessible

CONCLUSION

The ETHICS 2000 comments to Model Rule 1.6, and decisions under the Supreme Court Rules, generally apply traditional rules of confidentiality to new forms of communication and document storage. Thus, the practice at issue here can be compared to the storage of paper documents containing confidential client information in a warehouse operated by company or person outside the lawyer's direct control. In such a case, the same risk exists that an employee of the warehouse, or some other person, will access and perhaps disclose the information without authorization. But neither the Model Rules nor the Supreme Court Rules would prohibit the third party storage arrangement altogether. Rather, they require the attorney to act reasonably and competently to protect the information from inadvertent and unauthorized access and disclosure.

It is therefore the opinion of this committee that an attorney may use an outside agency to store confidential client information in electronic forms, and on hardware located outside the attorney's direct supervision and control, so long as the attorney observes the usual obligations applicable to such arrangements for third party storage services. If, for example, the attorney does not reasonably believe that the confidentiality will be preserved, or if the third party declines to agree to keep the information confidential, then the attorney violates SCR 156 by transmitting the data to the third party. But if the third party can be reasonably relied upon to maintain the confidentiality and agrees to do so, then the transmission is permitted by the rules even without client consent.

The client may consent to the storage of confidential information in any manner. It is clear that SCR 156 and the Supreme Court Rules generally would prefer that the lawyer obtain the client's informed consent before transmitting confidential information to third parties in

any case, but the rules do not prohibit the storage of electronic client information, without client consent, in any manner that complies with the lawyer's duty to competently and reasonably safeguard the confidentiality of client information.

NOTE: This opinion is issued by the Standing Committee on Ethics and Professional Responsibility of the State Bar of Nevada pursuant to SCR 225. It is advisory only. It is not binding on the courts, the State Bar of Nevada, its Board of Governors, any person or tribunal charged with regulatory responsibility, or any other member of the State Bar of Nevada.