90 PRESERVATION OF CLIENT CONFIDENCES IN VIEW OF MODERN COMMUNICATIONS TECHNOLOGY

Adopted November 14, 1992, revised July 2018.

Introduction

In recent years, there have been significant advances in communications technology. In addition, the cost of many modern communications methods and devices has been decreasing such that the use of email and of smartphones and other hand-held devices to communicate has become commonplace. It can be expected that new and improved communications methods and devices will continue to be developed.[1] A lawyer's use of these communications methods and devices carries the increased risk of inadvertent or unauthorized disclosure of information relating to the representation of a client. Therefore, lawyers must be mindful of their duty under Rule 1.6 of the Colorado Rules of Professional Conduct (Colo. RPC) "to make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."

Summary of Opinion

A lawyer's duty to make reasonable efforts to prevent misuse of client information extends to the exercise of reasonable care when selecting and using communications methods and devices.

1.This opinion is not intended to be a technical guide, and lawyers are encouraged to conduct their own research into the security of their communications devices before using them in the course of confidential communications.

Analysis

One of the most basic and time-honored precepts of the practice of law is that communications between a lawyer and a client are confidential. Colo. RPC 1.6, cmt. [2]. It necessarily follows that a lawyer has a duty use reasonable efforts to protect the confidentiality of such communications from inadvertent or unauthorized disclosure, or unauthorized access; and this duty is codified in Colo. RPC 1.6(c), which states: "A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." Comment [18] to Colo. RPC 1.6 explains: "The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure." The comment adds: "Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (*e.g.*, by making a device or important piece of software excessively difficult to use)."

Ever-increasing varieties of communications methods and devices are available for a lawyer's use, such as cloud-based email and smartphones. It is reasonable to expect that, in the future, there will continue to be technological advances that will both facilitate the communication of information and increase the possibility of inadvertent or unauthorized disclosure of, or unauthorized access to, such communications, as well as technological advances that will enhance a lawyer's ability to protect against such disclosure.

For instance, emails are now in widespread use. The American Bar Association Standing Committee on Ethics and Professional Responsibility (the ABA Standing Committee) has determined that using unencrypted email for professional correspondence is acceptable because it poses no greater risks than other communication modes that lawyers commonly use. ABA Comm. on Ethics and Prof. Resp., Formal Op. 99-413,"Protecting the Confidentiality of Unencrypted E-Mail" (1999). Various state ethics opinions have similarly concluded that, ordinarily, a lawyer's transmission of confidential information by

unencrypted email does not *per se* violate the lawyer's duty to maintain client confidentiality. *See, e.g.*, DC. Bar Ass'n, Ethics Op. 281, "Transmission of Confidential Information by Electronic Mail" (1998); Pa. Bar Ass'n Comm. on Legal Ethics and Prof. Resp., Op. 2011-200,"Ethical Obligations for Attorneys Using Cloud Computing/Software as a Service While Fulfilling the Duties of Confidentiality and Preservation of Client Property" (2011).

In 2017 the ABA Standing Committee issued a new opinion updating its Opinion 99-413. It found that unencrypted emails continue to be acceptable if a lawyer "has implemented basic and reasonably available methods of common electronic security measures," but added that "particularly strong protective measures, like encryption, are warranted in some circumstances." The Committee said that lawyers must use "a fact-specific approach to business security obligations that requires a 'process' to assess risks, identify and implement appropriate security measures responsive to those risks, verify that they are effectively implemented, and ensure that they are continually updated in response to new developments." ABA Comm. on Ethics and Prof. Resp., Formal Op. 477R,"Securing Communication of Protected Client Information" (2017).[2]

This Committee agrees that transmission of confidential information by unencrypted email does not *per se* violate Colo. RPC 1.6(c). As Comment [19] to that rule explains, the duty to take reasonable precautions to prevent confidential information from coming into the hands of unintended recipients "does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of [confidentiality]." Because email communications methods ordinarily afford a reasonable expectation of confidentiality, a lawyer's use of email for routine communications with clients does not *per se* violate Rule 1.6, if the lawyer has implemented basic and reasonably available methods of common electronic security measures.[3] Special circumstances, however, may warrant special precautions: For example, in appropriate circumstances

---

2.*See generally*, Eli Wald, "Legal Ethics' Next Frontier: Lawyers and Cybersecurity," 19 Chapman L. Rev. 501, 508-511 (2016) (discussing cybersecurity plans).

3.ABA Opinion 477R includes a useful discussion of "basic and reasonably available methods of common electronic security measures" as of 2017, when that opinion was issued.

lawyers who email highly sensitive confidential information should encrypt the communication. *See* Colo. RPC 1.6, cmts. [18], [19].

Smartphones have also become ubiquitous. As with email, because the use of smartphones usually affords a reasonable expectation of confidentiality, the mere use of a smartphone to have a voice conversation relating to the representation of a client does not violate Rule 1.6(c). *See* State Bar of Ariz. Comm. on Rules of Prof'l Conduct, Formal Op. 95-11,"Confidentiality; Cellular Phones" (1995) ("[T]he time has not yet come when a lawyer's mere use of a cellular phone to communicate with the client constitutes an ethical breach."); Del. State Bar Ass'n Comm. on Prof'l Ethics, Formal Op. 2001-2, (2001) (finding that use of a mobile phone is permissible unless "extraordinary circumstances" make disclosure likely); Minn. Law. Prof'l Resp. Bd., Op. 19,"Using Technology to Communicate Confidential Information to Clients" (1999) (opining that use of digital cordless and cellular phones or e-mail, even unencrypted, is permissible).

While the use of email or of smartphones and other such devices does not *per se* violate Rule 1.6(c), lawyers who take advantage of these communications technologies must make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, communications containing confidential client information, including adopting processes to assess and address cyber risks. For example, lawyers who access email on their laptops or smartphones using insecure or vulnerable public wireless Internet connections or in public places must take reasonable precautions to prevent the information from coming into the hands of unintended recipients, possibly including precautions such as encryption and strong password protection, as well as device disablement in the event their devices are hacked, lost, or stolen.

While the measures necessary to protect confidential information will vary based upon the technologies and infrastructures that each lawyer uses, and while the Committee acknowledges that the advances in technology make it difficult to provide specific standards that will apply to every lawyer, nevertheless there are common procedures and safeguards that lawyers should employ. Reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client may include the following: (i) "documentation of security practices and controls to instill a

culture of security" within a law firm;[4] (ii) periodic inspection of the lawyer's and, if applicable, the firm's email system for signs of cyber attacks and data theft; (iii) the use of basic cybersecurity measures, including using up-to-date virus scanners and firewalls,[5] installing patches and updates, using strong passwords updated from time to time, and eschewing the use of public cloud providers or file-sharing services for sharing documents; and (iv) the adoption of training protocols for lawyers and staff within a law firm.[6] *See* Colo. RPC 5.1, 5.3.

The frequency of advances in technology notwithstanding, Colorado lawyers "should keep abreast of . . . changes in communications and other relevant technologies," Colo. RPC 1.1 cmt. [8], so that they can make reasonable efforts to prevent inadvertent or unauthorized disclosure of, or unauthorized access to, confidential information as result of their use of communications technology. Lawyers have always had a duty to select modes and devices for communication that maintain the confidential nature of information related to the representation of clients. Just as a lawyer would not use a megaphone to communicate confidential information across a crowded intersection, so must the lawyer use reasonable care in selecting and using any mode of telecommunication in order not to unreasonably compromise representation-related information.

Lawyers using email, smartphones, or other electronic communications methods or devices should be aware of the risk that unauthorized persons may access confidential communications transmitted over those devices unless reasonable care is employed in their use. The mere inclusion of a "confidentiality notice," as is typically added to email messages, is not a substitute for reasonable care in ascertaining the correct email address of the intended recipient and accurately typing into an email's "send to" field to guard against

---

4.Kenneth N. Rashbaum, "Cybersecurity for Law Firms: Business Imperatives Update 2017," N.Y.L.J., vol. 257, no. 42, p. 14, Mar. 6, 2017.

5.Cal. State Bar Comm. on Prof. Resp. and Conduct, Formal Op. 2010-179,"Confidentiality and Technology" (2010) (an attorney using public wireless connections to conduct research and send e-mails should use precautions, such as personal firewalls and encrypting files and transmissions, or else risk violating his or her confidentiality and competence obligations).

6.Pa. Bar Ass'n Comm. on Legal Ethics and Prof'l Resp., Formal Op. 2011-200,"Ethical Obligations for Attorneys Using Cloud Computing/Software as a Service While Fulfilling the Duties of Confidentiality and Preservation of Client Property" (2011).

unintended transmission to the wrong person. Similarly, when leaving a land-line or cell-phone message containing representation-related information, a lawyer must exercise reasonable care to ensure that the message has been left for the intended recipient and that only the intended recipient will have access to it.

In the context of their duty to make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of their clients, lawyers must carefully consider the methods they, their associates, and their staff members utilize for the communication of representation-related information. Some new communications methods or devices may not provide a reasonable expectation of confidentiality. The lawyer has a duty to select communication methods and devices that are not likely to result in the unintentional disclosure of protected information. Moreover, when the lawyer knows or has reason to know that the client (or anyone else conveying confidential information to the lawyer or receiving it from the lawyer with respect to a client) has initiated a communication via a medium that is subject to relatively easy interception, Rule 1.6 might require the lawyer to warn that person about the risk of unintended disclosure. Further, lawyers should exercise care in using mobile devices such as smartphones and laptops in public places where others may easily overhear their conversations or see their transmissions.

Rule 1.4 directs a lawyer to promptly inform the client of any decision or circumstance with respect to which the client's informed consent is required by the Colorado Rules of Professional Conduct, to reasonably consult with the client about the means by which the client's objectives are to be accomplished, and to explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation. Colo. RPC 1.4(a)(1), (a)(2), (b). While it is not necessary to communicate every minute detail related to a client's representation,"[t]he client should have sufficient information to participate intelligently in decisions concerning the objectives of the representation and the means by which they are to be pursued" (Colo. RPC 1.4, cmt. [5]); and this duty to communicate and explain may apply to communications technology employed in the representation. Comment [18] to Rule 1.6 states, "A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule." For example, some highly sensitive matters may necessitate discussing the risks of public

wireless connections with the client if the lawyer intends to utilize such connections or, in the alternative, avoiding their use altogether. *See* Cal. Op. 2010-179.[7]

Conclusion

It is impossible to predict how technological advances will affect the confidentiality of client-lawyer communications effected by electronic means. However, regardless of technological developments, the lawyer must make reasonable efforts to guard against the risk that the medium of the communication the lawyer or the client employs may somehow compromise the confidential nature of the information being communicated.

7.Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as Colorado and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, e.g., Colorado's Data Breach Law, C.R.S. § 6-1-716, is beyond the scope of this opinion.