THE PROFESSIONAL ETHICS COMMITTEE
FOR THE STATE BAR OF TEXAS
Opinion No. 648

April 2015

QUESTION PRESENTED

Under the Texas Disciplinary Rules of Professional Conduct, may a lawyer communicate confidential information by email?

STATEMENT OF FACTS

Lawyers in a Texas law firm represent clients in family law, employment law, personal injury, and criminal law matters. When they started practicing law, the lawyers typically delivered written communication by facsimile or the U.S. Postal Service. Now, most of their written communication is delivered by web-based email, such as unencrypted Gmail.

Having read reports about email accounts being hacked and the National Security Agency obtaining email communications without a search warrant, the lawyers are concerned about whether it is proper for them to continue using email to communicate confidential information.

DISCUSSION

The Texas Disciplinary Rules of Professional Conduct do not specifically address the use of email in the practice of law, but they do provide for the protection of confidential information, defined broadly by Rule 1.05(a) to include both privileged and unprivileged client information, which might be transmitted by email.

Rule 1.05(b) provides that, except as permitted by paragraphs (c) and (d) of the Rule:

> "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." A determination of whether a lawyer violates the Disciplinary Rules, as opposed to fiduciary obligations, the law, or best practices, by sending an email containing confidential information, requires a case-by-case evaluation of whether that lawyer knowingly revealed confidential information to a person who was not permitted to receive that information under Rule 1.05.

The concern about sending confidential information by email is the risk that an unauthorized person will gain access to the confidential information. While this Committee has not addressed the propriety of communicating confidential information by email, many other ethics committees have, concluding that, in general, and except in special circumstances, the use of email, including unencrypted email, is a proper method of communicating confidential information. See, e.g., ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 99-413 (1999); ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 11-459 (2011); State Bar of Cal. Standing Comm. on Prof'l Responsibility and Conduct, Formal Op. 2010-179 (2010); Prof'l Ethics Comm. of the Maine Bd. of Overseers of the Bar, Op. No. 195 (2008); N.Y. State Bar Ass'n Comm. on Prof'l Ethics, Op. 820 (2008); Alaska Bar Ass'n Ethics Comm., Op. 98-2 (1998); D.C. Bar Legal Ethics Comm., Op. 281 (1998); Ill. State Bar Ass'n Advisory Opinion on Prof'l Conduct, Op. 96-10 (1997); State Bar Ass'n of N.D. Ethics Comm., Op. No. 97-09 (1997); S.C. Bar Ethics Advisory Comm., Ethics Advisory Op. 97-08 (1997); Vt. Bar Ass'n, Advisory Ethics Op. No 97-05 (1997).

Those ethics opinions often make two points in support of the conclusion that email communication is proper. First, the risk an unauthorized person will gain access to confidential information is inherent in the delivery of any written communication including delivery by the U.S. Postal Service, a private mail service, a courier, or facsimile. Second, persons who use email have a reasonable expectation of privacy based, in part, upon statutes that make it a crime to intercept emails. See, e.g., Alaska Bar Ass'n Ethics Comm. Op. 98-2 (1998); D.C. Bar Legal Ethics Comm., Op. 281 (1998). The statute cited in those opinions is the Electronic Communication Privacy Act (ECPA), which makes it a crime to

intercept electronic communication, to use the contents of the intercepted email, or to disclose the contents of intercepted email. 18 U.S.C. § 2510 *et seq.* Importantly, the statute provides that "[n]o otherwise privileged . . . electronic communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character." 18 U.S.C. § 2517(4).

The ethics opinions from other jurisdictions are instructive, as is Texas Professional Ethics Committee Opinion 572 (June 2006). The issue in Opinion 572 was whether a lawyer may, without the client's express consent, deliver the client's privileged information to a copy service hired by the lawyer to perform services in connection with the client's representation. Opinion 572 concluded that a lawyer may disclose privileged information to an independent contractor if the lawyer reasonably expects that the independent contractor will not disclose or use such items or their contents except as directed by the lawyer and will otherwise respect the confidential character of the information.

In general, considering the present state of technology and email usage, a lawyer may communicate confidential information by email. In some circumstances, however, a lawyer should consider whether the confidentiality of the information will be protected if communicated by email and whether it is prudent to use encrypted email or another form of communication. Examples of such circumstances are:

> 1. communicating highly sensitive or confidential information via email or unencrypted email connections;
> 2. sending an email to or from an account that the email sender or recipient shares with others;
> 3. sending an email to a client when it is possible that a third person (such as a spouse in a divorce case) knows the password to the email account, or to an individual client at that client's work email account, especially if the email relates to a client's employment dispute with his employer (see ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 11-459 (2011));
> 4. sending an email from a public computer or a borrowed computer or where the lawyer knows that the emails the lawyer sends are being read on a public or borrowed computer or on an unsecure network;
> 5. sending an email if the lawyer knows that the email recipient is accessing the email on devices that are potentially accessible to third persons or are not protected by a password; or
> 6. sending an email if the lawyer is concerned that the NSA or other law enforcement agency may read the lawyer's email communication, with or without a warrant.

In the event circumstances such as those identified above are present, to prevent the unauthorized or inadvertent disclosure of confidential information, it may be appropriate for a lawyer to advise and caution a client as to the dangers inherent in sending or accessing emails from computers accessible to persons other than the client. A lawyer should also consider whether circumstances are present that would make it advisable to obtain the client's informed consent to the use of email communication, including the use of unencrypted email. See Texas Rule 1.03(b) and ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 11-459 (2011). Additionally, a lawyer's evaluation of the lawyer's email technology and practices should be ongoing as there may be changes in the risk of interception of email communication over time that would indicate that certain or perhaps all communications should be sent by other means.

Under Rule 1.05, the issue in each case is whether a lawyer who sent an email containing confidential information knowingly revealed confidential information to a person who was not authorized to receive the information. The answer to that question depends on the facts of each case. Since a "knowing" disclosure can be based on actual knowledge or can be inferred, each lawyer must decide whether he or she has a reasonable expectation that the confidential character of the information will be maintained if the lawyer transmits the information by email.

This opinion discusses a lawyer's obligations under the Texas Disciplinary Rules of Professional Conduct, but it does not address other issues such as a lawyer's fiduciary obligations or best practices with respect to email communications. Furthermore, it does not address a lawyer's obligations under various statutes, such as the Health Insurance Portability and Accountability Act (HIPAA), which may impose other duties.

CONCLUSION

Under the Texas Disciplinary Rules of Professional Conduct, and 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.