AMERICAN BAR ASSOCIATION

STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 11-459 **August 4, 2011**

Duty to Protect the Confidentiality of E-mail Communications with One's Client

A lawyer sending or receiving substantive communications with a client via e-mail or other electronic means ordinarily must warn the client about the risk of sending or receiving electronic communications using a computer or other device, or e-mail account, where there is a significant risk that a third party may gain access. In the context of representing an employee, this obligation arises, at the very least, when the lawyer knows or reasonably should know that the client is likely to send or receive substantive client-lawyer communications via e-mail or other electronic means, using a business device or system under circumstances where there is a significant risk that the communications will be read by the employer or another third party.[1]

Introduction

Lawyers and clients often communicate with each other via e-mail and sometimes communicate via other electronic means such as text messaging. The confidentiality of these communications may be jeopardized in certain circumstances. For example, when the client uses an employer's computer, smartphone or other telecommunications device, or an employer's e-mail account to send or receive e-mails with counsel, the employer may obtain access to the e-mails. Employers often have policies reserving a right of access to employees' e-mail correspondence via the employer's e-mail account, computers or other devices, such as smartphones and tablet devices, from which their employees correspond. Pursuant to internal policy, the employer may be able to obtain an employee's communications from the employer's e-mail server if the employee uses a business e-mail address, or from a workplace computer or other employer-owned telecommunications device on which the e-mail is stored even if the employee has used a separate, personal e-mail account. Employers may take advantage of that opportunity in various contexts, such as when the client is engaged in an employment dispute or when the employer is monitoring employee e-mails as part of its compliance responsibilities or conducting an internal investigation relating to the client's work.[2] Moreover, other third parties may be able to obtain access to an employee's electronic communications by issuing a subpoena to the employer. Unlike conversations and written communications, e-mail communications may be permanently available once they are created.

The confidentiality of electronic communications between a lawyer and client may be jeopardized in other settings as well. Third parties may have access to attorney-client e-mails when the client receives or sends e-mails via a public computer, such as a library or hotel computer, or via a borrowed computer. Third parties also may be able to access confidential communications when the client uses a computer or other device available to others, such as when a client in a matrimonial dispute uses a home computer to which other family members have access.

In contexts such as these, clients may be unaware of the possibility that a third party may gain access to their personal correspondence and may fail to take necessary precautions. Therefore, the risk that third parties may obtain access to a lawyer's e-mail communications with a client raises the question of what, if any, steps a lawyer must take to prevent such access by third parties from occurring. This opinion addresses this question in the following hypothetical situation.

An employee has a computer assigned for her exclusive use in the course of her employment. The company's written internal policy provides that the company has a right of access to all employees' computers and e-mail files, including those relating to employees' personal matters. Notwithstanding this

---

[1] This opinion is based on the ABA Model Rules of Professional Conduct as amended by the ABA House of Delegates through August 2011. The laws, court rules, regulations, rules of professional conduct, and opinions promulgated in individual jurisdictions are controlling.

[2] Companies conducting internal investigations often secure and examine the e-mail communications and computer files of employees who are thought to have relevant information.

policy, employees sometimes make personal use of their computers, including for the purpose of sending personal e-mail messages from their personal or office e-mail accounts. Recently, the employee retained a lawyer to give advice about a potential claim against her employer. When the lawyer knows or reasonably should know that the employee may use a workplace device or system to communicate with the lawyer, does the lawyer have an ethical duty to warn the employee about the risks this practice entails?

Discussion

Absent an applicable exception, Rule 1.6(a) requires a lawyer to refrain from revealing "information relating to the representation of a client unless the client gives informed consent." Further, a lawyer must act competently to protect the confidentiality of clients' information. This duty, which is implicit in the obligation of Rule 1.1 to "provide competent representation to a client," is recognized in two Comments to Rule 1.6. Comment [16] observes that 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." Comment [17] states in part: "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.... 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."

This Committee has recognized that these provisions of the Model Rules require lawyers to take reasonable care to protect the confidentiality of client information,[3] including information contained in e-mail communications made in the course of a representation. In ABA Op. 99-413 (1999) ("Protecting the Confidentiality of Unencrypted E-Mail"), the Committee concluded that, in general, a lawyer may transmit information relating to the representation of a client by unencrypted e-mail sent over the Internet without violating Model Rule 1.6(a) because the mode of transmission affords a reasonable expectation of privacy from a technological and legal standpoint. The opinion, nevertheless, cautioned lawyers to consult with their clients and follow their clients' instructions as to the mode of transmitting highly sensitive information relating to the clients' representation. It found that particularly strong protective measures are warranted to guard against the disclosure of highly sensitive matters.

Clients may not be afforded a "reasonable expectation of privacy" when they use an employer's computer to send e-mails to their lawyers or receive e-mails from their lawyers. Judicial decisions illustrate the risk that the employer will read these e-mail communications and seek to use them to the employee's disadvantage. Under varying facts, courts have reached different conclusions about whether an employee's client-lawyer communications located on a workplace computer or system are privileged, and the law appears to be evolving.[4] This Committee's mission does not extend to interpreting the substantive law, and

---

[3] *See, e.g.*, ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 08-451 (2008) (Lawyer's Obligations When Outsourcing Legal and Nonlegal Support Services) ("the obligation to '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'" requires a lawyer outsourcing legal work "to recognize and minimize the risk that any outside service provider may inadvertently -- or perhaps even advertently -- reveal client confidential information to adverse parties or to others who are not entitled to access ... [and to] verify that the outside service provider does not also do work for adversaries of their clients on the same or substantially related matters.").

[4] *See, e.g.*, Stengart v. Loving Care Agency, Inc., 990 A.2d 650, 663 (N.J. 2010) (privilege applied to e-mails with counsel using "a personal, password protected e-mail account" that were accessed on a company computer); Sims v. Lakeside Sch., No. C06-1412RSM, 2007 WL 2745367, at *2 (W.D. Wash. Sept. 20, 2007) (privilege applied to web-based e-mails to and from employee's counsel on hard drive of computer furnished by employer); National Econ. Research Assocs. v. Evans, No. 04–2618–BLS2, 21 Mass.L.Rptr. 337, 2006 WL 2440008, at *5 (Mass. Super. Aug. 3, 2006) (privilege applied to "attorney-client communications unintentionally stored in a temporary file on a company-owned computer that were made via a private, password-protected e-mail account accessed through the Internet, not the company's Intranet"); Holmes v. Petrovich Development Co., 191 Cal.App.4th 1047, 1068-72 (2011) (privilege

therefore we express no view on whether, and in what circumstances, an employee's communications with counsel from the employee's workplace device or system are protected by the attorney-client privilege. Nevertheless, we consider the ethical implications posed by the risks that these communications will be reviewed by others and held admissible in legal proceedings.[5] Given these risks, a lawyer should ordinarily advise the employee-client about the importance of communicating with the lawyer in a manner that protects the confidentiality of e-mail communications, just as a lawyer should avoid speaking face-to-face with a client about sensitive matters if the conversation might be overheard and should warn the client against discussing their communications with others. In particular, as soon as practical after a client-lawyer relationship is established, a lawyer typically should instruct the employee-client to avoid using a workplace device or system for sensitive or substantive communications, and perhaps for any attorney-client communications, because even seemingly ministerial communications involving matters such as scheduling can have substantive ramifications.

The time at which a lawyer has an ethical obligation under Rules 1.1 and 1.6 to provide advice of this nature will depend on the circumstances. At the very least, in the context of representing an employee, this ethical obligation arises when the lawyer knows or reasonably should know that the client is likely to send or receive substantive client-lawyer communications via e-mail or other electronic means,[6] using a business device or system under circumstances where there is a significant risk that the communications will be read by the employer or another third party. Considerations tending to establish an ethical duty to protect client-lawyer confidentiality by warning the client against using a business device or system for substantive e-mail communications with counsel include, but are not limited to, the following: (1) that the client has engaged in, or has indicated an intent to engage in, e-mail communications with counsel; (2) that the client is employed in a position that would provide access to a workplace device or system; (3) that, given the circumstances, the employer or a third party has the ability to access the e-mail communications; and (4) that, as far as the lawyer knows, the employer's internal policy and the jurisdiction's laws do not clearly protect the privacy of the employee's personal e-mail communications via a business device or system. Unless a lawyer has reason to believe otherwise, a lawyer ordinarily should assume that an employer's internal policy allows for access to the employee's e-mails sent to or from a workplace device or system.

The situation in the above hypothetical is a clear example of where failing to warn the client about the risks of e-mailing communications on the employer's device can harm the client, because the employment dispute would give the employer a significant incentive to access the employee's workplace e-mail and the employer's internal policy would provide a justification for doing so. The obligation arises once the lawyer has reason to believe that there is a significant risk that the client will conduct e-mail communications with the lawyer using a workplace computer or other business device or via the employer's e-mail account. This possibility ordinarily would be known, or reasonably should be known, at the outset of the representation. Given the nature of the representation–an employment dispute–the lawyer is on notice that the employer may search the client's electronic correspondence. Therefore, the lawyer must ascertain, unless the answer is already obvious, whether there is a significant risk that the client will use a business e-mail address for personal communications or whether the employee's position entails using an employer's device. Protective measures would include the lawyer refraining from sending e-mails

---

inapplicable to communications with counsel using workplace computer); Scott v. Beth Israel Medical Center, Inc., 847 N.Y.S.2d 436, 440-43 (N.Y. Sup. Ct. 2007) (privilege inapplicable to employer's communications with counsel via employer's e-mail system); Long v. Marubeni Am. Corp., No. 05CIV.639(GEL)(KNF), 2006 WL 2998671, at *3-4 (S.D.N.Y. Oct. 19, 2006) (e-mails created or stored in company computers were not privileged, notwithstanding use of private password-protected e-mail accounts); Kaufman v. SunGard Inv. Sys., No. 05-CV-1236 (JLL), 2006 WL 1307882, at *4 (D.N.J. May 10, 2006) (privilege inapplicable to communications with counsel using employer's network).

[5] For a discussion of a lawyer's duty when receiving a third party's e-mail communications with counsel, *see* ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 11-460 (2011) (Duty when Lawyer Receives Copies of a Third Party's E-mail Communications with Counsel).

[6] This opinion principally addresses e-mail communications, which are the most common way in which lawyers communicate electronically with clients, but it is equally applicable to other means of electronic communications.

to the client's workplace, as distinct from personal, e-mail address,[7] and cautioning the client against using a business e-mail account or using a personal e-mail account on a workplace computer or device at least for substantive e-mails with counsel.

As noted at the outset, the employment scenario is not the only one in which attorney-client electronic communications may be accessed by third parties. A lawyer sending or receiving substantive communications with a client via e-mail or other electronic means ordinarily must warn the client about the risk of sending or receiving electronic communications using a computer or other device, or e-mail account, to which a third party may gain access. The risk may vary. Whenever a lawyer communicates with a client by e-mail, the lawyer must first consider whether, given the client's situation, there is a significant risk that third parties will have access to the communications. If so, the lawyer must take reasonable care to protect the confidentiality of the communications by giving appropriately tailored advice to the client.

[7] Of course, if the lawyer becomes aware that a client is receiving personal e-mail on a workplace computer or other device owned or controlled by the employer, then a duty arises to caution the client not to do so, and if that caution is not heeded, to cease sending messages even to personal e-mail addresses.