THE STATE BAR OF CALIFORNIA
STANDING COMMITTEE ON
PROFESSIONAL RESPONSIBILITY AND CONDUCT
FORMAL OPINION NO. 2010-179

ISSUE: Does an attorney violate the duties of confidentiality and competence he or she owes to a client by using technology to transmit or store confidential client information when the technology may be susceptible to unauthorized access by third parties?

DIGEST: Whether an attorney violates his or her duties of confidentiality and competence when using technology to transmit or store confidential client information will depend on the particular technology being used and the circumstances surrounding such use. Before using a particular technology in the course of representing a client, an attorney must take appropriate steps to evaluate: 1) the level of security attendant to the use of that technology, including whether reasonable precautions may be taken when using the technology to increase the level of security; 2) the legal ramifications to a third party who intercepts, accesses or exceeds authorized use of the electronic information; 3) the degree of sensitivity of the information; 4) the possible impact on the client of an inadvertent disclosure of privileged or confidential information or work product; 5) the urgency of the situation; and 6) the client's instructions and circumstances, such as access by others to the client's devices and communications.

AUTHORITIES INTERPRETED: Rules 3-100 and 3-110 of the California Rules of Professional Conduct.

Business and Professions Code section 6068, subdivision (e)(1).

Evidence Code sections 917(a) and 952.

STATEMENT OF FACTS

Attorney is an associate at a law firm that provides a laptop computer for his use on client and firm matters and which includes software necessary to his practice. As the firm informed Attorney when it hired him, the computer is subject to the law firm's access as a matter of course for routine maintenance and also for monitoring to ensure that the computer and software are not used in violation of the law firm's computer and Internet-use policy. Unauthorized access by employees or unauthorized use of the data obtained during the course of such maintenance or monitoring is expressly prohibited. Attorney's supervisor is also permitted access to Attorney's computer to review the substance of his work and related communications.

Client has asked for Attorney's advice on a matter. Attorney takes his laptop computer to the local coffee shop and accesses a public wireless Internet connection to conduct legal research on the matter and email Client. He also takes the laptop computer home to conduct the research and email Client from his personal wireless system.

DISCUSSION

Due to the ever-evolving nature of technology and its integration in virtually every aspect of our daily lives, attorneys are faced with an ongoing responsibility of evaluating the level of security of technology that has increasingly become an indispensable tool in the practice of law. The Committee's own research – including conferring with computer security experts – causes it to understand that, without appropriate safeguards (such as firewalls, secure username/password combinations, and encryption), data transmitted wirelessly can be intercepted and read with increasing ease. Unfortunately, guidance to attorneys in this area has not kept pace with technology. Rather than engage in a technology-by-technology analysis, which would likely become obsolete shortly, this

opinion sets forth the general analysis that an attorney should undertake when considering use of a particular form of technology.

1. The Duty of Confidentiality

In California, attorneys have an express duty "[t]o maintain inviolate the confidence, and at every peril to himself or herself to preserve the secrets, of his or her client."[1/] (Bus. & Prof. Code, § 6068, subd. (e)(1).) This duty arises from the relationship of trust between an attorney and a client and, absent the informed consent of the client to reveal such information, the duty of confidentiality has very few exceptions. (Rules Prof. Conduct, rule 3-100 & discussion ["[A] member may not reveal such information except with the consent of the client or as authorized or required by the State Bar Act, these rules, or other law."].)[2/]

Unlike Rule 1.6 of the Model Rules of Professional Conduct ("MRPC"), the exceptions to the duty of confidentiality under rule 3-100 do not expressly include disclosure "impliedly authorized in order to carry out the representation." (MRPC, Rule 1.6.) Nevertheless, the absence of such language in the California Rules of Professional Conduct does not prohibit an attorney from using postal or courier services, telephone lines, or other modes of communication beyond face-to-face meetings, in order to effectively carry out the representation. There is a distinction between actually disclosing confidential information to a third party for purposes ancillary to the representation,[3/] on the one hand, and using appropriately secure technology provided by a third party as a method of communicating with the client or researching a client's matter,[4/] on the other hand.

Section 952 of the California Evidence Code, defining "confidential communication between client and lawyer" for purposes of application of the attorney-client privilege, includes disclosure of information to third persons "to whom disclosure is reasonably necessary for the transmission of the information or the accomplishment of the purpose for which the lawyer is consulted." (Evid. Code, § 952.) While the duty to protect confidential client information is broader in scope than the attorney-client privilege (Discussion [2] to rule 3-100; *Goldstein v. Lees* (1975) 46 Cal.App.3d 614, 621, fn. 5 [120 Cal.Rptr. 253]), the underlying principle remains the same, namely, that transmission of information through a third party reasonably necessary for purposes of the representation should not be deemed to have destroyed the confidentiality of the information. (See Cal. State Bar Formal Opn. No. 2003-161 [repeating the Committee's prior observation "that the duty of confidentiality and the evidentiary privilege share the same basic policy foundation: to encourage clients to disclose all possibly pertinent information to their attorneys so that the attorneys may effectively represent the clients' interests."].) Pertinent here, the manner in which an attorney acts to safeguard confidential client information is governed by the duty of competence, and determining whether a third party has the ability to access and use confidential client information in a manner that is unauthorized by the client is a subject that must be considered in conjunction with that duty.

2. The Duty of Competence

Rule 3-110(A) prohibits the intentional, reckless or repeated failure to perform legal services with competence. Pertinent here, "competence" may apply to an attorney's diligence and learning with respect to handling matters for clients. (Rules Prof. Conduct, rule 3-110(B).) The duty of competence also applies to an attorney's "duty to supervise the work of subordinate attorney and non-attorney employees or agents." (Discussion to rule 3-110.)

1/ "Secrets" include "[a]ny 'information gained in the professional relationship that the client has requested be held inviolate or the disclosure of which would be embarrassing or would likely be detrimental to the client.'" (Cal. State Bar Formal Opn. No. 1981-58.)

2/ Unless otherwise indicated, all future references to rules in this opinion will be to the Rules of Professional Conduct of the State Bar of California.

3/ In this regard, compare Cal. State Bar Formal Opn. No. 1971-25 (use of an outside data processing center without the client's consent for bookkeeping, billing, accounting and statistical purposes, if such information includes client secrets and confidences, would violate section 6068, subdivision (e)), with Los Angeles County Bar Assn. Formal Opn. No. 374 (1978) (concluding that in most circumstances, if protective conditions are observed, disclosure of client's secrets and confidences to a central data processor would not violate section 6068(e) and would be the same as disclosures to non-lawyer office employees).

4/ Cf. Evid. Code, § 917(b) ("A communication … does not lose its privileged character for the sole reason that it is communicated by electronic means or because persons involved in the delivery, facilitation, or storage of electronic communication may have access to the content of the communication.").

With respect to acting competently to preserve confidential client information, the comments to Rule 1.6 of the MRPC[5/] provide:

> [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. See Rules 1.1, 5.1 and 5.3.
>
> [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.

(MRPC, cmts. 16 & 17 to Rule 1.6.) In this regard, the duty of competence includes taking appropriate steps to ensure both that secrets and privileged information of a client remain confidential and that the attorney's handling of such information does not result in a waiver of any privileges or protections.

3. Factors to Consider

In accordance with the duties of confidentiality and competence, an attorney should consider the following before using a specific technology:[6/]

a) The attorney's ability to assess the level of security afforded by the technology, including without limitation:

   i) Consideration of how the particular technology differs from other media use. For example, while one court has stated that, "[u]nlike postal mail, simple e-mail generally is not 'sealed' or secure, and can be accessed or viewed on intermediate computers between the sender and recipient (unless the message is encrypted)" (*American Civil Liberties Union v. Reno* (E.D.Pa. 1996) 929 F.Supp. 824, 834, aff'd (1997) 521 U.S. 844 [117 S.Ct. 2329]), most bar associations have taken the position that the risks of a third party's unauthorized review of email (whether by interception or delivery to an unintended recipient) are similar to the risks that confidential client information transmitted by standard mail service will be opened by any of the many hands it passes through on the way to its recipient or will be misdirected[7/] (see, e.g., ABA Formal Opn. No. 99-413[8/] [concluding that attorneys have a reasonable expectation of privacy in email communications, even if unencrypted, "despite some risk of interception and disclosure"]; Los Angeles County Bar Assn. Formal Opn. No. 514 (2005) ["Lawyers are not required

---

[5/] In the absence of on-point California authority and conflicting state public policy, the MRPC may serve as guidelines. (*City & County of San Francisco v. Cobra Solutions, Inc.* (2006) 38 Cal. 4th 839, 852 [43 Cal.Rptr.3d 771].)

[6/] These factors should be considered regardless of whether the attorney practices in a law firm, a governmental agency, a non-profit organization, a company, as a sole practitioner or otherwise.

[7/] Rule 1-100(A) provides that "[e]thics opinions and rules and standards promulgated by other jurisdictions and bar associations may . . . be considered" for professional conduct guidance.

[8/] In 1999, the ABA Committee on Ethics and Professional Responsibility reviewed state bar ethics opinions across the country and determined that, as attorneys' understanding of technology has improved, the opinions generally have transitioned from concluding that use of Internet email violates confidentiality obligations to concluding that use of unencrypted Internet email is permitted without express client consent. (ABA Formal Opn. No. 99-413 [detailing various positions taken in state ethics opinions from Alaska, Washington D.C., Kentucky, New York, Illinois, North Dakota, South Carolina, Vermont, Pennsylvania, Arizona, Iowa and North Carolina].)

to encrypt e-mail containing confidential client communications because e-mail poses no greater risk of interception and disclosure than regular mail, phones or faxes."]; Orange County Bar Assn. Formal Opn. No. 97-0002 [concluding use of encrypted email is encouraged, but not required].) (See also *City of Reno v. Reno Police Protective Assn.* (2003) 118 Nev. 889, 897-898 [59 P.3d 1212] [referencing an earlier version of section 952 of the California Evidence Code and concluding "that a document transmitted by e-mail is protected by the attorney-client privilege as long as the requirements of the privilege are met."].)

ii) Whether reasonable precautions may be taken when using the technology to increase the level of security.[9/] As with the above-referenced views expressed on email, the fact that opinions differ on whether a particular technology is secure suggests that attorneys should take reasonable steps as a precautionary measure to protect against disclosure.[10/] For example, depositing confidential client mail in a secure postal box or handing it directly to the postal carrier or courier is a reasonable step for an attorney to take to protect the confidentiality of such mail, as opposed to leaving the mail unattended in an open basket outside of the office door for pick up by the postal service. Similarly, encrypting email may be a reasonable step for an attorney to take in an effort to ensure the confidentiality of such communications remain so when the circumstance calls for it, particularly if the information at issue is highly sensitive and the use of encryption is not onerous. To place the risks in perspective, it should not be overlooked that the very nature of digital technologies makes it easier for a third party to intercept a much greater amount of confidential information in a much shorter period of time than would be required to transfer the same amount of data in hard copy format. In this regard, if an attorney can readily employ encryption when using public wireless connections and has enabled his or her personal firewall, the risks of unauthorized access may be significantly reduced.[11/] Both of these tools are readily available and relatively inexpensive, and may already be built into the operating system. Likewise, activating password protection features on mobile devices, such as laptops and PDAs, presently helps protect against access to confidential client information by a third party if the device is lost, stolen or left unattended. (See David Ries & Reid Trautz, *Law Practice Today*, "Securing Your Clients' Data While On the Road," October 2008 [noting reports that "as many as 10% of laptops used by American businesses are stolen during their useful lives and 97% of them are never recovered"].)

iii) Limitations on who is permitted to monitor the use of the technology, to what extent and on what grounds. For example, if a license to use certain software or a technology service imposes a requirement of third party access to information related to the attorney's use of the technology, the attorney may need to confirm that the terms of the requirement or authorization do not permit the third party to disclose confidential client information to others or use such information for any purpose other than to ensure the functionality of the software or that the technology is not being used for an improper purpose, particularly if the information at issue is highly sensitive.[12/] "Under Rule 5.3 [of the MRPC], a lawyer retaining such an outside service provider is required to make reasonable efforts to ensure that

---

[9/] Attorneys also should employ precautions to protect confidential information when in public, such as ensuring that the person sitting in the adjacent seat on an airplane cannot see the computer screen or moving to a private location before discussing confidential information on a mobile phone.

[10/] Section 60(1)(b) of the Restatement (Third) of The Law Governing Lawyers provides that "a lawyer must take steps reasonable in the circumstances to protect confidential client information against impermissible use or disclosure by the lawyer's associates or agents that may adversely affect a material interest of the client or otherwise than as instructed by the client."

[11/] Similarly, this Committee has stated that if an attorney is going to maintain client documents in electronic form, he or she must take reasonable steps to strip any metadata containing confidential information of other clients before turning such materials over to a current or former client or his or her new attorney. (See Cal. State Bar Formal Opn. 2007-174.)

[12/] A similar approach might be appropriate if the attorney is employed by a non-profit or governmental organization where information may be monitored by a person or entity with interests potentially or actually in conflict with the attorney's client. In such cases, the attorney should not use the technology for the representation, absent informed consent by the client or the ability to employ safeguards to prevent access to confidential client information. The attorney also may need to consider whether he or she can competently represent the client without the technology.

the service provider will not make unauthorized disclosures of client information. Thus when a lawyer considers entering into a relationship with such a service provider he must ensure that the service provider has in place, or will establish, reasonable procedures to protect the confidentiality of information to which it gains access, and moreover, that it fully understands its obligations in this regard. [Citation.] In connection with this inquiry, a lawyer might be well-advised to secure from the service provider in writing, along with or apart from any written contract for services that might exist, a written statement of the service provider's assurance of confidentiality." (ABA Formal Opn. No. 95-398.)

Many attorneys, as with a large contingent of the general public, do not possess much, if any, technological savvy. Although the Committee does not believe that attorneys must develop a mastery of the security features and deficiencies of each technology available, the duties of confidentiality and competence that attorneys owe to their clients do require a basic understanding of the electronic protections afforded by the technology they use in their practice. If the attorney lacks the necessary competence to assess the security of the technology, he or she must seek additional information or consult with someone who possesses the necessary knowledge, such as an information technology consultant.[13/] (Cf. Rules Prof. Conduct, rule 3-110(C) ["If a member does not have sufficient learning and skill when the legal service is undertaken, the member may nonetheless perform such services competently by 1) associating with or, where appropriate, professionally consulting another lawyer reasonably believed to be competent, or 2) by acquiring sufficient learning and skill before performance is required."].)

b) Legal ramifications to third parties of intercepting, accessing or exceeding authorized use of another person's electronic information. The fact that a third party could be subject to criminal charges or civil claims for intercepting, accessing or engaging in unauthorized use of confidential client information favors an expectation of privacy with respect to a particular technology. (See, e.g., 18 U.S.C. § 2510 et seq. [Electronic Communications Privacy Act of 1986]; 18 U.S.C. § 1030 et seq. [Computer Fraud and Abuse Act]; Pen. Code, § 502(c) [making certain unauthorized access to computers, computer systems and computer data a criminal offense]; Cal. Pen. Code, § 629.86 [providing a civil cause of action to "[a]ny person whose wire, electronic pager, or electronic cellular telephone communication is intercepted, disclosed, or used in violation of [Chapter 1.4 on Interception of Wire, Electronic Digital Pager, or Electronic Cellular Telephone Communications]."]; *eBay, Inc. v. Bidder's Edge, Inc.* (N.D.Cal. 2000) 100 F.Supp.2d 1058, 1070 [in case involving use of web crawlers that exceeded plaintiff's consent, court stated "[c]onduct that does not amount to a substantial interference with possession, but which consists of intermeddling with or use of another's personal property, is sufficient to establish a cause of action for trespass to chattel."].)[14/]

c) The degree of sensitivity of the information. The greater the sensitivity of the information, the less risk an attorney should take with technology. If the information is of a highly sensitive nature and there is a risk of disclosure when using a particular technology, the attorney should consider alternatives unless the client provides informed consent.[15/] As noted above, if another person may have access to the communications transmitted between the attorney and the client (or others necessary to the representation), and may have an interest in the information being disclosed that is in conflict with the client's interest, the attorney should take precautions to ensure that the person will not be able to access the information or should avoid using the technology. These types of situations increase the likelihood for intrusion.

[13/] Some potential security issues may be more apparent than others. For example, users of unsecured public wireless connections may receive a warning when accessing the connection. However, in most instances, users must take affirmative steps to determine whether the technology is secure.

[14/] Attorneys also have corresponding legal and ethical obligations not to invade the confidential and privileged information of others.

[15/] For the client's consent to be informed, the attorney should fully advise the client about the nature of the information to be transmitted with the technology, the purpose of the transmission and use of the information, the benefits and detriments that may result from transmission (both legal and nonlegal), and any other facts that may be important to the client's decision. (Los Angeles County Bar Assn. Formal Opn. No. 456 (1989).) It is particularly important for an attorney to discuss the risks and potential harmful consequences of using the technology when seeking informed consent.

d) Possible impact on the client of an inadvertent disclosure of privileged or confidential information or work product, including possible waiver of the privileges.[16/] Section 917(a) of the California Evidence Code provides that "a communication made in confidence in the course of the lawyer-client, physician-patient, psychotherapist-patient, clergy-penitent, husband-wife, sexual assault counselor-victim, or domestic violence counselor-victim relationship … is presumed to have been made in confidence and the opponent of the claim of privilege has the burden of proof to establish that the communication was not confidential." (Evid. Code, § 917(a).) Significantly, subsection (b) of section 917 states that such a communication "does not lose its privileged character for the sole reason that it is communicated by electronic means or because persons involved in the delivery, facilitation, or storage of electronic communication may have access to the content of the communication." (Evid. Code, § 917(b). See also Penal Code, § 629.80 ["No otherwise privileged communication intercepted in accordance with, or in violation of, the provisions of [Chapter 1.4] shall lose its privileged character."]; 18 U.S.C. § 2517(4) ["No otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of [18 U.S.C. § 2510 et seq.] shall lose its privileged character."].) While these provisions seem to provide a certain level of comfort in using technology for such communications, they are not a complete safeguard. For example, it is possible that, if a particular technology lacks essential security features, use of such a technology could be deemed to have waived these protections. Where the attorney-client privilege is at issue, failure to use sufficient precautions may be considered in determining waiver.[17/] Further, the analysis differs with regard to an attorney's duty of confidentiality. Harm from waiver of attorney-client privilege is possible depending on if and how the information is used, but harm from disclosure of confidential client information may be immediate as it does not necessarily depend on use or admissibility of the information, including as it does matters which would be embarrassing or would likely be detrimental to the client if disclosed.

e) The urgency of the situation. If use of the technology is necessary to address an imminent situation or exigent circumstances and other alternatives are not reasonably available, it may be reasonable in limited cases for the attorney to do so without taking additional precautions.

f) Client instructions and circumstances. If a client has instructed an attorney not to use certain technology due to confidentiality or other concerns or an attorney is aware that others have access to the client's electronic devices or accounts and may intercept or be exposed to confidential client information, then such technology should not be used in the course of the representation.[18/]

4. Application to Fact Pattern[19/]

In applying these factors to Attorney's situation, the Committee does not believe that Attorney would violate his duties of confidentiality or competence to Client by using the laptop computer because access is limited to authorized individuals to perform required tasks. However, Attorney should confirm that personnel have been appropriately instructed regarding client confidentiality and are supervised in accordance with rule 3-110. (See *Crane v. State Bar* (1981) 30 Cal.3d 117, 123 [177 Cal.Rptr. 670] ["An attorney is responsible for the work product of his employees which is performed pursuant to his direction and authority."]; *In re Complex Asbestos Litig.* (1991) 232 Cal.App.3d 572, 588 [283 Cal.Rptr. 732] [discussing law firm's ability to supervise employees and ensure they protect client confidences]; Cal. State Bar Formal Opn. No. 1979-50 [discussing lawyer's duty to explain to

---

16/ Consideration of evidentiary issues is beyond the scope of this opinion, which addresses only the ethical implications of using certain technologies.

17/ For example, with respect to the impact of inadvertent disclosure on the attorney-client privilege or work-product protection, rule 502(b) of the Federal Rules of Evidence states: "When made in a Federal proceeding or to a Federal office or agency, the disclosure does not operate as a waiver in a Federal or State proceeding if: 1. the disclosure is inadvertent; 2. the holder of the privilege or protection took reasonable steps to prevent disclosure; and 3. the holder promptly took reasonable steps to rectify the error, including (if applicable) following Federal Rule of Civil Procedure 26(b)(5)(B)." As a practical matter, attorneys also should use appropriate confidentiality labels and notices when transmitting confidential or privileged client information.

18/ In certain circumstances, it may be appropriate to obtain a client's informed consent to the use of a particular technology.

19/ In this opinion, we are applying the factors to the use of computers and wireless connections to assist the reader in understanding how such factors function in practice. Use of other electronic devices would require similar considerations.

employee what obligations exist with respect to confidentiality].) In addition, access to the laptop by Attorney's supervisor would be appropriate in light of her duty to supervise Attorney in accordance with rule 3-110 and her own fiduciary duty to Client to keep such information confidential.

With regard to the use of a public wireless connection, the Committee believes that, due to the lack of security features provided in most public wireless access locations, Attorney risks violating his duties of confidentiality and competence in using the wireless connection at the coffee shop to work on Client's matter unless he takes appropriate precautions, such as using a combination of file encryption, encryption of wireless transmissions and a personal firewall.[20/] Depending on the sensitivity of the matter, Attorney may need to avoid using the public wireless connection entirely or notify Client of possible risks attendant to his use of the public wireless connection, including potential disclosure of confidential information and possible waiver of attorney-client privilege or work product protections, and seek her informed consent to do so.[21/]

Finally, if Attorney's personal wireless system has been configured with appropriate security features,[22/] the Committee does not believe that Attorney would violate his duties of confidentiality and competence by working on Client's matter at home. Otherwise, Attorney may need to notify Client of the risks and seek her informed consent, as with the public wireless connection.

CONCLUSION

An attorney's duties of confidentiality and competence require the attorney to take appropriate steps to ensure that his or her use of technology in conjunction with a client's representation does not subject confidential client information to an undue risk of unauthorized disclosure. Because of the evolving nature of technology and differences in security features that are available, the attorney must ensure the steps are sufficient for each form of technology being used and must continue to monitor the efficacy of such steps.

This opinion is issued by the Standing Committee on Professional Responsibility and Conduct of the State Bar of California. It is advisory only. It is not binding upon the courts, the State Bar of California, its Board of Governors, any persons, or tribunals charged with regulatory responsibilities, or any member of the State Bar.

[20/] Local security features available for use on individual computers include operating system firewalls, antivirus and antispam software, secure username and password combinations, and file permissions, while network safeguards that may be employed include network firewalls, network access controls such as virtual private networks (VPNs), inspection and monitoring. This list is not intended to be exhaustive.

[21/] Due to the possibility that files contained on a computer may be accessed by hackers while the computer is operating on an unsecure network connection and when appropriate local security features, such as firewalls, are not enabled, attorneys should be aware that *any* client's confidential information stored on the computer may be at risk regardless of whether the attorney has the file open at the time.

[22/] Security features available on wireless access points will vary and should be evaluated on an individual basis.