THE STATE BAR OF CALIFORNIA
STANDING COMMITTEE ON
PROFESSIONAL RESPONSIBILITY AND CONDUCT
FORMAL OPINION INTERIM NO. 08-0002

ISSUES: Does an attorney violate the duties of confidentiality and competence he or she owes to a client by: 1) using a computer to which the organization employing the attorney and its supervisors have access; 2) using computer software to which the software developer has access; or 3) using a public or home wireless connection?

DIGEST: To comply with his or her duties of confidentiality and competence, an attorney must take appropriate steps to evaluate: 1) the level of security attendant to the use of a particular technology in the course of representing a client; 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; and 5) whether reasonable precautions may be taken when using the technology to increase the level of security. With regard to use of a computer to which the organization employing the attorney and its supervisors have access, the attorney must consider the purpose of, and limitations on, the access and whether the organization itself or an individual with access may have an interest in the information that is in conflict with the client's interest. The attorney may need to take precautions to ensure that any interested persons will not be able to access the information or, absent informed client consent, the attorney may need to consider whether he or she can competently represent the client without using the computer in connection with the representation. With regard to access to confidential information by a software developer, the attorney may use the software as long as the attorney does not have a reason to believe the information will be used improperly. However, he or she may need to discuss the issue with the client to determine appropriate methods of proceeding if the information at issue is highly sensitive or the software developer has an adverse interest in the matter. With regard to use of a public or home wireless connection, the attorney risks violating his or her duties of confidentiality and competence unless appropriate precautions are taken, such as using an adequate encryption device and a personal firewall. Depending on the situation, including if the information at issue is of a highly sensitive nature, the attorney may need to avoid using the wireless connection entirely, or notify the client of possible risks associated with use of the wireless connection and seek the client's informed consent to do so. Generally, the attorney should not use an unsecured public wireless connection that does not require a password for access.

AUTHORITIES INTERPRETED:

Rule 3-100 of the Rules of Professional Conduct of the State Bar of California.

Rule 3-110 of the Rules of Professional Conduct of the State Bar of California.

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

STATEMENT OF FACTS

A non-profit organization provides a variety of services to the low-income community in which it is located, including job training, child care, and a free medical clinic. The organization is supported through contributions from the religious community and individuals, as well as public grants and contracts. The organization recently began providing free and low-cost legal services to its clientele. Although the organization has one executive

director, each of the units operates independently and has a separate unit head. Attorney A, who has been practicing law for two years, was hired by the organization to assist low-income community members with legal issues. He reports to Attorney B, who is the unit head for the legal services unit. Attorney A uses a laptop computer provided by the organization, which includes software necessary to his practice. The computer provided by the organization is subject to the organization's access as a matter of course, pursuant to notices received at the time of his hire, for routine maintenance and monitoring by appropriate personnel to ensure that the computer and software are not being used for accessing improper websites or other personal use. Any unauthorized access by employees of the organization or unauthorized use of the data obtained during the course of such maintenance or monitoring is expressly prohibited. Attorney B, as Attorney A's supervisor, is also permitted access to Attorney A's computer to review the substance of his work and related communications. In addition, the licenses for the software provide that, as a condition of use, the software developer is permitted to obtain certain data from the computer to assist it in troubleshooting and to enable it to provide offers and services tailored to the user.

Client X has asked for Attorney A's advice regarding a potential claim for damage to her property against a public figure in the community. Attorney A works in a large, open room in the legal services unit of the organization, and all unit heads have access privileges to the non-profit organization's records for operational purposes only. To ensure that no one at the non-profit organization observes his research concerning Client X's claim, Attorney A 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 X. He also takes the laptop computer home to conduct the research and email Client X from his personal wireless system.

DISCUSSION

Due to the ever-evolving nature of technology and its integration in virtually every aspect 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. <u>The Duty of Confidentiality</u>

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

---

[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.

actually disclosing confidential information to a third party for purposes ancillary to the representation,[3/] on the one hand, and using appropriate secure technology provided by a third party as a method of communicating with the client or researching a client's matter, 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,[4/] 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. <u>The Duty of Competence</u>

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 a matter for a client. (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.)

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

---

[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 (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/] The duty of confidentiality applies to all information gained in the course of the attorney-client relationship, regardless of the source, if the client has asked that the information be kept secret or if disclosure would likely harm or embarrass the client. (*Goldstein v. Lees* (1975) 46 Cal.App.3d 614, 621, fn. 5 [120 Cal.Rptr. 253]; Cal. State Bar Formal Opn. Nos. 2003-161, 1993-133, 1986-87, and 1981-58.)

[5/] In situations where California authorities do not address the particular conduct at issue, courts may look to the MRPC for an appropriate standard. (*City & County of San Francisco v. Cobra Solutions, Inc.* (2006) 38 Cal. 4th 839, 852 [43 Cal.Rptr.3d 771]; *In re National Mortgage Equity Corp. Mortgage Pool Certificates Sec. Litig.* (C.D. Cal. 1988) 120 F.R.D. 687, 690-691.)

> 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.

Therefore, before using a certain technology, an attorney should consider the following:

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 email 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* (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 (see, e.g., ABA Formal Opn. No. 99-413[6/] [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 ["Lawyers are not required 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 [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) Limitations on who is permitted to monitor the use of the technology, to what extent and on what grounds. For example, if an employer or a license to use certain software or a technology service includes a required authorization to allow a third party access to information related to the attorney's use of the technology, the attorney must confirm that the terms of the 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. Further, if the information may be monitored by a third party or an attorney's employer with interests potentially or actually in conflict with the client, then the attorney should not use the technology for the representation, absent informed consent by the client or the ability to employ safeguards to prevent the third party's or employer's access to confidential client information. In such a situation, the attorney also should consider whether he or she can competently represent the client without the technology.

   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

---

[6/] 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].)

consultant.[7/] (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 of intercepting, accessing or exceeding authorized use of 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]."]; *Quon v. Arch Wireless Operating Co.* (C.D.Cal. 2004) 309 F.Supp.2d 1204, 1210-1211 [invasion of privacy claim under California Constitution stated where provider of pager service released police officers' electronic text messages to city officials]; *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."].)

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.[8/] Likewise, 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, such as the attorney's internet service provider who is adverse to the client, the attorney should take precautions to ensure that the person will not be able to access the information or should avoid using the technology.

d) Possible impact on the client of an inadvertent disclosure of privileged or confidential information or work product, including possible waiver of the privileges.[9/] 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]

[7/] 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.

[8/] 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.) It is particularly important for an attorney to discuss the risks and potential harmful consequences of using the technology when seeking informed consent. Further, an advance waiver of confidentiality is not per se improper; to the extent the waiver is "informed," it is valid. (Cal. State Bar Formal Opn. No. 1989-115.)

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

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 this provision seems to provide a certain level of comfort in using technology for such communications, it is 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. Further, where the attorney-client privilege is at issue, failure to use sufficient precautions may be considered in determining intent to disclose,[10/] but the same analysis does not apply in terms of complying with 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) Whether reasonable precautions may be taken when using the technology to increase the level of security.[11/] For example, if an attorney can readily employ an encryption device when using public wireless connections and has enabled his or her personal firewall, the risks of unauthorized access may be significantly reduced.[12/] Both of these tools are readily available and relatively inexpensive, and may already be built in to the operating system.

f) 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.

3. <u>Application to Fact Pattern</u>[13/]

In applying these factors to Attorney A's situation, the Committee does not believe that Attorney A would violate his duties of confidentiality or competence to Client X by using the laptop computer because the organization's authorized access is expressly limited to routine maintenance and monitoring to ensure that the computer and software are not being used for accessing improper websites or other personal use. Although the organization contains units that do not perform legal services, access is limited to certain individuals who perform the required tasks and, therefore, their review would be no different than review by information technology or administrative employees of law firms. However, Attorney A should confirm that the 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 employee what obligations exist with respect to confidentiality].)

Due to the interest or curiosity others outside the legal services unit may express in a claim against a public figure, Attorney A should take steps at the outset to ensure that the other unit heads' access privileges to the information on Attorney A's laptop computer are restricted during the representation of Client X, or take appropriate precautions to

---

[10/] As a practical matter, attorneys also should use appropriate confidentiality labels and notices when transmitting confidential or privileged client information.

[11/] Attorneys should employ similar 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.

[12/] 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.)

[13/] In this opinion we are applying the factors to the use of computers. Use of other electronic devices would require similar considerations.

prevent such unit heads' access during Attorney A's representation of Client X, such as the use of password protection or features that limit access to certain files to specified individuals. If Attorney A is unable to implement adequate precautions, absent informed client consent to Attorney A's use of the laptop computer despite the risks of disclosure, Attorney A must consider whether he can competently represent Client X without using the laptop computer in connection with the representation. In contrast, Attorney B's access to the laptop would be entirely appropriate in light of her duty to supervise Attorney A in accordance with rule 3-110 and her own fiduciary duty to Client X to keep such information confidential.

With regard to the licensed software, the Committee does not believe that Attorney A's use of such software in connection with the representation of Client X would violate his duties of confidentiality or competence, as long as Attorney A does not have a reason to believe the information will be used improperly. Because the details of how software licenses permit or limit access or use of information gathered from the user are often not readily apparent or ascertainable, Attorney A may need to discuss the issue with Client X to decide on the appropriate method of proceeding if the information at issue is of a highly sensitive nature or the software developer has an adverse interest in the matter.

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 A risks violating his duties of confidentiality and competence in using the wireless connection at the coffee shop to work on Client X's matter unless he takes appropriate precautions, such as using an adequate encryption device and a personal firewall.[14/] Further, Attorney A generally should not use any unsecured public wireless connection that does not require a password for access. Depending on the situation, including if the information at issue is of a highly sensitive nature, Attorney A may need to avoid using the public wireless connection entirely or notify Client X 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.[15/]

Finally, if Attorney A's personal wireless system has been configured with appropriate security features,[16/] the Committee does not believe that Attorney A would violate his duties of confidentiality and competence by working on Client X's matter at home. Otherwise, Attorney A may need to notify Client X 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.

[14/] 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, inspection and monitoring. This list is not intended to be exhaustive.

[15/] 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.

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