Session Date: Friday, May 19, 2023

Session Time: 10:00am-11:15am

Session Name: Protecting Your Cards: Data Breaches and eDiscovery Lessons

Total Minutes: 75

Total Credit Hours: 1.25

Protecting Your Cards:
Data Breaches and eDiscovery Lessons

Panelists:

Hon. Ronald H. Sargis
U.S. Bankruptcy Judge; Eastern District of California

Caroline R. Djang
Shareholder; Buchalter, A Professional Corporation

Joseph R. Dunn
Member; Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, P.C.

Producers:

Maria J. Cho
Associate; Faegre Drinker Biddle & Reath LLP

Matthew J. Olson
Of Counsel; Dorsey & Whitney LLP

Table of Contents

The repealed prior version of this rule that was effective from November 1, 2018 to March 22, 2021, and the Executive Summary concerning those amendments can be found here.

Rule 1.1 Competence
(Rule Approved by the Supreme Court, Effective March 22, 2021)

(a) A lawyer shall not intentionally, recklessly, with gross negligence, or repeatedly fail to perform legal services with competence.

(b) For purposes of this rule, "competence" in any legal service shall mean to apply the (i) learning and skill, and (ii) mental, emotional, and physical ability reasonably* necessary for the performance of such service.

(c) If a lawyer does not have sufficient learning and skill when the legal services are undertaken, the lawyer nonetheless may provide competent representation by (i) associating with or, where appropriate, professionally consulting another lawyer whom the lawyer reasonably believes* to be competent, (ii) acquiring sufficient learning and skill before performance is required, or (iii) referring the matter to another lawyer whom the lawyer reasonably believes* to be competent.

(d) In an emergency a lawyer may give advice or assistance in a matter in which the lawyer does not have the skill ordinarily required if referral to, or association or consultation with, another lawyer would be impractical. Assistance in an emergency must be limited to that reasonably* necessary in the circumstances.

Comment

[1] The duties set forth in this rule include the duty to keep abreast of the changes in the law and its practice, including the benefits and risks associated with relevant technology.

[2] This rule addresses only a lawyer's responsibility for his or her own professional competence. See rules 5.1 and 5.3 with respect to a lawyer's disciplinary responsibility for supervising subordinate lawyers and nonlawyers.

[3] See rule 1.3 with respect to a lawyer's duty to act with reasonable* diligence.

THE STATE BAR OF CALIFORNIA
STANDING COMMITTEE ON
PROFESSIONAL RESPONSIBILITY AND CONDUCT
FORMAL OPINION NO. 2012-184

ISSUE: May an attorney maintain a virtual law office practice ("VLO") and still comply with her ethical obligations, if the communications with the client, and storage of and access to all information about the client's matter, are all conducted solely through the internet using the secure computer servers of a third-party vendor (i.e., "cloud computing")?

DIGEST: As it pertains to the use of technology, the Business and Professions Code and the Rules of Professional Conduct do not impose greater or different duties upon a VLO practitioner operating in the cloud than they do upon an attorney practicing in a traditional law office. While an attorney may maintain a VLO in the cloud where communications with the client, and storage of and access to all information about the client's matter, are conducted solely via the internet using a third-party's secure servers, Attorney may be required to take additional steps to confirm that she is fulfilling her ethical obligations due to distinct issues raised by the hypothetical VLO and its operation. Failure of Attorney to comply with all ethical obligations relevant to these issues will preclude the operation of a VLO in the cloud as described herein.

AUTHORITIES INTERPRETED: Rules 1-100, 1-300, 1-310, 3-100, 3-110, 3-310, 3-400, 3-500, 3-700, and 4-200 of the Rules of Professional Conduct of the State Bar of California.[1/]

Business and Professions Code section 6068, subdivisions (e), (m), and (n).

Business and Professions Code sections 6125, 6126, 6127, 6147, and 6148.

California Rules of Court, Rules 3.35-3.37 and 5.70-5.71.[2/]

STATEMENT OF FACTS

Attorney, a California licensed solo practitioner with a general law practice, wishes to establish a virtual law office (VLO).[3/] Attorney's target clients are low and moderate-income individuals who have access to the internet, looking for legal assistance in business transactions, family law, and probate law.

In her VLO, Attorney intends to communicate with her clients through a secure internet portal created on her website, and to both store, and access, all information regarding client matters through that portal. The information on the secure internet portal will be password protected and encrypted. Attorney intends to assign a separate password to each client after that client has registered and signed Attorney's standard engagement letter so that a particular client can access information relating to his or her matter only. Attorney plans not to communicate with her clients by phone, e-mail or in person, but to limit communications solely to the internet portal through a function that allows attorney and client to send communications directly to each other within the internet portal.

Attorney asks whether her contemplated VLO practice would satisfy all applicable ethics rules.

[1/] Unless otherwise noted, all rule references are to the Rules of Professional Conduct of the State Bar of California.

[2/] Rules 5.70-5.71 repealed effective January 1, 2013 is revised and renumbered as Rule 5.425 adopted effective January 1, 2013.

[3/] For a general discussion of virtual law practice, see Stephanie L. Kimbro, ABA Law Practice Management Section, "Virtual Law Practice" (2010) (ISBN 978-1-60442-828-5).

DISCUSSION

As a result of ever increasing innovations in technology, the world has moved significantly toward internet communications – through email, chats, blogs, social networking sites, and message boards. The legal services industry has not been untouched by these innovations and the use of technology, including the internet, is becoming more common, and even necessary, in the provision of legal services. Consistent with this trend, and with the benefits of convenience, flexibility, and cost reduction, the provision of legal services via a VLO has started to emerge as an increasingly viable vehicle in which to deliver accessible and affordable legal services to the general public.

The VLO, also variously known as Digital Law, Online Law, eLawyering and Lawfirm 2.0, may take many different forms. For the purposes of this opinion, "VLO" shall refer to the delivery of, and payment for,[4/] legal services exclusively, or nearly exclusively, through the law firm's portal on a website, where all of the processing, communication, software utilization, and computing will be internet-based. In the hypothetical VLO discussed in this opinion, a client's communication with the law firm, as well as his access to the legal services provided, is supplied by the firm through a secure internet portal provided by a third-party internet-based vendor, accessible by the client with a unique user name and access code specific to the client's particular matter only. The lawyer and client may not ever physically meet or even speak on a telephone.

The Committee recognizes that although VLOs exist and operate only through the use of relatively new technology, the use of such technology itself is not unique to this VLO; rather, many lawyers operating in traditional non-VLOs utilize some or many aspects of this same technology. The California Business and Professions Code and the Rules of Professional Conduct do not impose greater or different duties upon a VLO practitioner than they do upon a traditional non-VLO practitioner as it pertains to the use of technology. This opinion focuses on issues that the Committee believes are particularly implicated by the VLO's cloud-based nature described herein, although many of the same issues may arise in any law practice.[5/] For a fuller discussion on the analysis that the Committee believes an attorney should undertake when considering use of a particular form of technology, we refer the reader to California State Bar Formal Opinion No. 2010-179.

1. Attorney's Duty of Confidentiality in Our Hypothetical VLO Is the Same as That of an Attorney in a Traditional Non-VLO, But Requires Some Specific Due Diligence.

A lawyer has a duty to "maintain inviolate the confidence, and at every peril to himself or herself, preserve the secrets of his or her client." (Bus. & Prof. Code, § 6068(e)(1)). With certain limited exceptions, the client's confidential information may not be revealed absent the informed written consent of the client. (Rule 3-100(A); Cal. State Bar Formal Opn. No. 2010-179.)

[4/] Attorneys accepting credit card payment should consult Cal. State Bar Formal Opn. No. 2007-172.

[5/] The Committee recognizes that the fact situation presented in this opinion may raise an issue regarding the unauthorized practice of law – particularly where prospective clients from anywhere in the country (or, indeed, the world) easily may contact Attorney through her internet site. Rule 1-300(A) states that "[a] member shall not aid any person or entity in the unauthorized practice of law." However, this opinion is not intended to address or opine on the issue of the unauthorized practice of law. Regarding activities undertaken by an individual who is not an active member of the California State Bar, members should consider Business and Professions Code sections 6125-6127. Members should also consider rule 1-300 (Unauthorized Practice of Law) and rule 1-310 (Forming a Partnership with a Non-Lawyer). Regarding what constitutes the practice of law in California, members should consider the following cases: *Farnham v. State Bar* (1976) 17 Cal.3d 605 [131 Cal.Rptr. 661]; *Bluestein v. State Bar* (1974) 13 Cal.3d 162 [118 Cal.Rptr. 175]; *Baron v. City of Los Angeles* (1970) 2 Cal.3d 535 [86 Cal.Rptr. 673]; *Crawford v. State Bar* (1960) 54 Cal.2d 659 [7 Cal.Rptr. 746]; *People v. Merchants Protective Corporation* (1922) 189 Cal. 531, 535; *Birbrower, Montalbano, Condon & Frank v. Superior Ct.* (1998) 17 Cal.4th 119 [70 Cal.Rptr.2d 304]; *People v. Landlords Professional Services* (1989) 215 Cal.App.3d 1599 [264 Cal.Rptr. 548]; and *People v. Sipper* (1943) 61 Cal.App.2d Supp. 844 [142 P.2d 960]. Members of the State Bar of California should also consider how their VLO services might implicate rules and regulations regarding the unauthorized practice of law of other jurisdictions outside of California, if applicable.

In California State Bar Formal Opinion No. 2010-179, this Committee discussed the ethical confidentiality and competency concerns of a practitioner using technology in providing legal services, and the considerations an attorney should take into account when determining what reasonable steps would be necessary to comply with those obligations. While those obligations are the same for attorneys using technology both in a VLO and a traditional non-VLO,[6/] due to the *wholly outsourced* internet-based nature of our hypothetical VLO, special considerations are implicated which require specific due diligence on the part of our VLO practitioner.

This is because even though Attorney in this hypothetical is choosing an outside vendor, the fact of the outsourcing does not change Attorney's obligation to take reasonable steps to protect and secure the client's information. (Cal. State Bar Formal Opn. No. 2010-179; *see also* American Bar Association (ABA) Formal Opn. No. 08-451.)[7/] Attorney's compliance with her duty of confidentiality requires that she exercise reasonable due diligence both in the selection, and then in the continued use, of the VLO vendor. Attorney should determine that the VLO vendor selected by her employs policies and procedures that at a minimum equal what Attorney herself would do on her own to comply with her duty of confidentiality.[8/] This Committee has recognized that while Attorney is not required to become a technology expert in order to comply with her duty of confidentiality and competence, Attorney does owe her clients a duty to have a basic understanding of the protections afforded by the technology she uses in her practice. If Attorney lacks the necessary competence to assess the security of the technology, she must seek additional information, or consult with someone who possesses the necessary knowledge, such as an information technology consultant. (Rule 3-110(C); Cal. State Bar Formal Opn. No. 2010-179.) Only after Attorney takes these reasonable steps to understand the basic technology available and how it will work in this hypothetical VLO, and determines that her duty of confidentiality and competence can be met in the contemplated VLO, may Attorney proceed. Factors to consider when selecting a VLO vendor may include:

A. *Credentials of vendor.* ABA Formal Opn. No. 08-451; New York State Bar Assoc. Opinion 842.

B. *Data Security.* Cal. State Bar Formal Opn. No. 2010-179; ABA Formal Opn. No. 08-451, ABA Formal Opn. No. 95-398; eLawyering Task Force, Law Practice Management Section, "Suggested Minimum Requirements for Law Firms Delivering Legal Services Online" (2009); New York State Bar Assoc. Opinion 842; Penn. Bar Assoc. Formal Opinions 2010-200 and 2011-200.

[6/] Similarly, while this opinion addresses a VLO that exists only in a "cloud" setting – that is, on the internet, through a third-party vendor, where the services are provided wholly through and on the internet – the Committee understands that it is possible to have a VLO that can be accessed in a technology-based, but non-"cloud" setting. The special considerations discussed in this section of this opinion may not necessarily apply to such VLOs. A member must consider the specific circumstances of his or her VLO, particularly where information is hosted and by whom, to determine whether these considerations apply.

[7/] The ABA Model Rules are not binding in California but may be used for guidance by lawyers where there is no direct California authority and the ABA Model Rules do not conflict with California policy. *City & County of San Francisco v. Cobra Solutions, Inc.* (2006) 38 Cal.4th 839, 852. Thus, in the absence of related California authority, we may look to the Model Rules, and the ABA Formal Opinions interpreting them, as well as the ethics opinions of other jurisdictions or bar associations for guidance. (Rule 1-100(A) (ethics opinions and rules and standards promulgated by other jurisdictions and bar associations may also be considered); *State Compensation Ins. Fund v. WPS, Inc*. (1999) 70 Cal.App.4th 644, 656 [82 Cal.Rptr.2d 799].)

[8/] Even apart from a VLO and the use of technology, attorneys have a duty to take reasonable precautions to protect their client's confidential information. (Rule 3-100(A); Cal. State Bar Formal Opn. No. 2010-179.) For example, an attorney who keeps files both in paper form and on an internet server may employ the most up-to-date security precautions for his server, but then fail to lock the door to his office, thereby allowing anyone to come in and rifle through his clients' paper files. The duties an attorney assumes when he operates exclusively in the cloud are no different than the lawyer who exclusively prefers paper files – both must act competently and take reasonable steps to preserve their client's confidences. All that changes in a VLO is the steps the attorneys must take to meet this competence and confidentiality requirement.

C. *Vendor's Transmission of the Client's Information in the Cloud Across Jurisdictional Boundaries or Other Third-Party Servers.*[9/] ABA Formal. Opn. No. 08-451; Navetta and Forsheit, Information Law Group, Legal Implications of Cloud Computing (2009) series, parts 1, 2, and 3.

D. *Attorney's Ability to Supervise Vendor.* ABA Formal Opn. No. 08-451.

E. *Terms of Service of Contract with Vendor.* Rules Prof. Conduct, rules 3-100 and 3-700.

Even after Attorney satisfies herself that the security of the technology employed by the VLO provider is adequate to comply with her ethical obligations, Attorney should conduct periodic reassessments of all of these factors to confirm that the VLO vendor's services and systems remain at the level for which she initially contracted, and that changes in the vendor's business environment or management have not negatively affected its adequacy.[10/]

Finally, Attorney should consider whether her ethical obligations require that she make appropriate disclosures and obtain the client's consent to the fact that an outside vendor is providing the technological base of Attorney's law firm, and that, as a result, the outside vendor will be receiving and exclusively storing the client's confidential information. (ABA Formal Opn. No. 08-451; see also Cal. State Bar Formal Opn. No. 2010-179.) In that regard, compare California State Bar Formal Opinion No. 1971-25 (use of outside data processing center without client's consent for bookkeeping, billing, accounting, and statistical purposes, if such information includes client secrets and confidences, would violate section 6068(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).

In our hypothetical facts, Attorney's proposed VLO is password protected and encrypted, and each specific client will only be allowed access to his own matter. Assuming attorney has taken reasonable steps to determine that her duty of confidentiality and competence can be met, given the current standards of technology and security, such protections likely are sufficient in today's business environment. As technologies change, however, security standards also may change. Attorney, either directly or with the assistance of consultants, should keep abreast of the most current standards so that she can evaluate whether the measures taken by her firm's VLO provider to protect client confidentiality have not become outdated.

2. <u>The Online-Based Nature of Communication and Delivery of Legal Services Inherent in this VLO Raises Distinct Concerns As It Pertains to Attorney's Fulfillment of Her Duty of Competence.</u>

Just as the duty to maintain a client's confidences is one of the cornerstones of an attorney's duty of competence (rule 3-110), so too is the attorney's ability to effectively communicate with a client a prerequisite to affording competent counsel. (Rule 3-500; see also *Calvert v. State Bar* (1991) 54 Cal.3d 765, 782 [1 Cal.Rptr.2d 684] ("Adequate communication with clients is an integral part of competent professional performance as an attorney.").

[9/] Data stored and traveling in the cloud potentially travels across numerous jurisdictional boundaries, including international boundaries, as a matter of course. In some instances, the data may be designed from the outset to be stored on servers located outside of the United States. Third-party vendors may also subcontract out their work. When selecting and contracting with her VLO vendor, Attorney should address and minimize exposure of the client to legal issues triggered by both the international movement, and/or storage, of information in the cloud, and the potential subcontracting out of the vendor's services to unknown third-party vendors, which may impact confidentiality, without the prior written consent of Attorney and affected clients.

[10/] In the event Attorney determines that the third-party vendor fails to meet the confidentiality standards that Attorney believes necessary for her VLO to comply with her ethical responsibilities relating to information storage, Attorney may consider alternative situations to store the client information at issue, in a non-cloud-based setup, as long as the non-cloud based setup, as it relates to information storage and access to that stored information, each independently comply with Attorney's duty of confidentiality as discussed herein, and as set forth in California State Bar Formal Opinion No. 2010-179.

In our VLO, all services and communications are conducted wholly through the VLO portal on the internet, without any physical meeting, and without any one-on-one contact even by phone. While the Committee believes that such an internet-only, attorney-client relationship, under the right circumstances, can meet all of Attorney's ethical obligations, such an internet-only structure does raise distinct ethics issues as it pertains to communications and competency.

First, Attorney must take reasonable steps to set up her client intake system in such a way that she is receiving from the prospective client sufficient information to determine if she can provide the prospective legal services at issue.[11/] As an initial matter, Attorney should obtain sufficient information to conclude that the client in fact is the actual prospective client, or an authorized representative of the client, as opposed to someone acting without authority. Although an attorney in a non-VLO has this same obligation, the lack of face-to-face or even phone communication with the client in our hypothetical VLO may hinder Attorney's ability to make this determination, thereby potentially necessitating extra measures of assurance. Whether Attorney must take additional steps to confirm the prospective client's identity will depend on the circumstances of the representation and initial communications, and the information Attorney obtains from the prospective client.[12/]

Second, Attorney's intake procedures also must include her receipt of sufficient information to make the initial determination of whether she can perform the requested legal services competently in a VLO at all,[13/] or at least receipt of sufficient detailed information to determine whether the circumstances are such that further investigation is needed. *Butler v. State Bar* (1986) 42 Cal.3d 323, 329 [228 Cal.Rptr. 499].

Third, once Attorney determines that she has sufficient information to determine that she can provide the legal services at issue, on any matter which requires client understanding, Attorney must take reasonable steps to ensure that the client comprehends the legal concepts involved and the advice given, irrespective of the mode of communication used, so that the client is in a position to make an informed decision. (Cal. State Bar Formal Opn. No. 1984-77.) Attorney is not truly "communicating" with the client if the client does not understand what Attorney is saying – whether because of a language barrier or simply a lack of understanding of the legal concepts being discussed. This would be the case whether Attorney is communicating with the client in person, on the phone, by letter, or over the internet. In this hypothetical VLO, however, it may be more difficult for Attorney to form a reasonable belief that the client understands her, as Attorney will be without nonverbal cues (such as body language, eye contact, etc.) or even verbal clues (such as voice inflections or hesitations). Thus, Attorney may need to take additional reasonable steps to permit her to form a reasonable belief that she truly is "communicating" with her client.

In California State Bar Formal Opinion No. 1984-77, this Committee addressed the issue of client comprehension if an attorney has reason to doubt it, and specific steps that an attorney should take where the client does not speak the same language, or does so in a limited fashion. The opinion advises that an attorney providing services in a traditional law office to a client with little or no ability to communicate in English may need to communicate in the

---

[11/] Attorney's obligations on intake are the same as the usual obligations of a non-VLO on intake. See, e.g., Rules Prof. Conduct, rule 3-310 (conflicts of interest); Bus. & Prof. Code, §§ 6147, 6148 (engagement letters).

[12/] See for example, *Ethics Alert: Internet Scams Targeting Attorneys* (January 2011) The State Bar of California Committee on Professional Responsibility and Conduct <http://ethics.calbar.ca.gov/LinkClick.aspx?fileticket=z8N90vbh088%3d&tabid=834> (as of May 23, 2012).

[13/] The Committee recognizes that certain legal practices may be amenable to this type of VLO, while others likely are not. By way of example only, an attorney may be able to competently draft a simple will or provide tax advice over the internet without speaking with the client, but it is less likely that she can defend the client in litigation in this same manner. Still further, even within practice areas, or within specific matters, there are differing levels of complexity that can alter the permissibility of using the VLO for delivery of the services. This opinion does not define specifically what practices can or cannot work under this type of cloud-based VLO. Instead, attorneys are cautioned that they should make an individual matter-by-matter analysis as to whether they can fulfill their duty to act competently in a VLO, first, as to the type of matter involved generally, and, second, as to the specific aspects of that given matter. Only when the answer to both inquiries is affirmative may Attorney proceed under a cloud-based VLO as described herein.

client's particular language or dialect, or use a skilled interpreter. Attorney must likewise confirm that the client has sufficient skills in the language being used by Attorney. Written internet-based communications between Attorney and the client may demonstrate the client's understanding. However, a third party may be communicating on behalf of a client who does not understand the language in question or is not literate in that language. Attorney may wish to take further steps to confirm the client's level of comprehension.

Fourth, once Attorney begins the representation, she must keep the client reasonably informed about significant developments relating to the representation, including promptly complying with reasonable requests for information and copies of significant documents. (Bus. & Prof. Code, § 6068(m) & (n); rule 3-500.) To the extent Attorney's process for informing the client is merely posting the information in the internet portal, Attorney must take reasonable steps to determine that the client in fact is receiving the information in a timely manner. Attorney also may wish to emphasize to the client throughout the representation the importance of checking into the portal regularly to get updates, and to establish an alternative method of communication in the event the portal does not work effectively to reach the client in a timely manner. If Attorney is not reasonably convinced that she is effectively and timely communicating with the client in the hypothetical VLO, and that the client understands what is being communicated, then Attorney may not proceed with the VLO representation as contemplated.

Fifth, given that individuals have varied understanding of technology and how to use it, attorneys using a VLO must have a reasonable basis to believe that the client has sufficient access to technology and the ability necessary to communicate through Attorney's web-based portal, just as the non-VLO attorney must have a reasonable basis to believe that the client can understand her on the phone, read and understand her written correspondence, or otherwise have an ability to communicate with her.

Sixth, if after her initial intake, Attorney concludes that she cannot competently deliver legal services to the client through this VLO, Attorney must decline to undertake that representation within this VLO context. (Rule 3-110.) If legal services already have commenced when Attorney determines she cannot competently continue to deliver legal services to the client through this VLO, Attorney must cease further representation through this VLO. (Rule 3-700.)[14/] In that circumstance, Attorney may choose instead to undertake or continue the prospective legal services in a traditional non-VLO, if she has the proper traditional non-VLO structure to do so, and if the traditional methods of delivering legal services cure the problems of competency raised by this VLO. At a minimum, even if Attorney determines that she should withdraw, consistent with rule 3-700, she must continue to competently provide legal services to the client until such withdrawal is both ethically permissible and complete. Such continued representation must include non-VLO services, such as telephone or in-person communications, if such services are reasonable steps to avoid reasonably foreseeable prejudice to the rights of the client. (Rule 3-700(A)(2).)

Alternatively, in the situation where competency problems arise due to the complexity of the legal matter at issue, if narrowing the scope of legal services to be provided in the VLO would be permissible and also cure those competency problems, Attorney may do so and proceed through the VLO. In this circumstance, the material change in scope of representation must be communicated to and accepted by the client and Attorney. (See ABA Formal Opn. No. 11-458.)[15/] Before undertaking a limited scope representation, Attorney should consider the various restrictions on such representations.[16/] Even under a permissible limited scope representation, Attorney should still

---

[14/] Rule 3-700(D) requires that, upon termination of the attorney-client employment, subject to any protective order or nondisclosure agreement, an attorney shall promptly release to the client, at the request of the client, all of the client papers and property. In our VLO, all the data is electronic and should be in a format to which Attorney has, by contract with the third-party vendor, already arranged for access – both for her and for the client – even after Attorney terminates the relationship with the third-party vendor for that particular matter. Upon client request, Attorney must release to the client the electronic versions of *all* papers and property in question, at Attorney's expense, after first stripping each document of any and all metadata that contains confidential information belonging to other clients. (Cal. State Bar Formal Opn. No. 2007-174.)

[15/] In narrowing the scope of representation, Attorney must satisfy herself that the fee arrangements with the client remains reasonable and continues to comply with Rule 4-200, and if not, make the necessary adjustments with the client.

[16/] See Cal. Rules of Court, Rules 3.35-3.37 (limited scope representation in general civil cases); ABA Model Rule 1.2(c) and Comments (6)-(8) (lawyer may limit scope of representation provided limitation is reasonable and the

advise the client (a) what services are not being undertaken; (b) what services still will need to be done, including advice that there may be other remedies that Attorney will not investigate or pursue; (c) what risks to the client, if any, could result from the limitation of the scope of representation; and (d) that other counsel should be consulted as to those matters not undertaken by the present counsel. (*Nichols v. Keller* (1993) 15 Cal.App.4th 1672, 1683-1684 [19 Cal.Rptr.2d 601] ("even when a retention is expressly limited, the attorney may still have a duty to alert the client to legal problems which are reasonably apparent, even though they fall outside the scope of the retention"); ABA Model Rule 1.2(c).)

Finally, in all law offices, including this hypothetical VLO, attorneys have a duty to supervise subordinate attorneys, and non-attorney employees or agents. (Rule 3-110 (discussion par. 1); *Crane v. State Bar* (1981) 30 Cal.3d 117, 123 [177 Cal.Rptr. 670] (rejecting contention that attorney's rules violations were "precipitated by members of his staff"); *Henderson v. Pacific Gas & Electric Co.* (2010) 187 Cal.App.4th 215, 218 [113 Cal.Rptr.3d 692] ("Although an attorney cannot be held responsible for every detail of office procedure, it is an attorney's responsibility to supervise the work of his or her staff members."); see also ABA Model Rule 5.1.) In our hypothetical VLO, supervision can be a challenge if Attorney and her various subordinate attorneys and employees operate out of several different physical locations. Whatever method Attorney chooses to comply with her duty to supervise, Attorney must take reasonable measures to ascertain that everyone under her supervision is complying with the Rules of Professional Conduct, including the duties of confidentiality and competence, notwithstanding any physical separation.

CONCLUSION

The Business and Professions Code and the Rules of Professional Conduct do not impose greater or different duties upon a VLO practitioner operating in the cloud than they do upon attorneys practicing in a traditional non-VLO. While Attorney may maintain a VLO in the cloud, Attorney may be required to take additional steps to confirm that she is reasonably addressing ethical concerns raised by issues distinct to this type of VLO. Failure by Attorney to comply with her ethical obligations relevant to these issues will preclude the operation of a VLO in the cloud as described.

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.

*[**Publisher's Note:** Internet resources cited in this opinion were last accessed by staff on May 23, 2012. Copies of these resources are on file with the State Bar's Office of Professional Competence.]*

---

client gives informed consent); see also *In the Matter of Valinoti* (Review Dept. 2002) 4 Cal. State Bar Ct. Rptr. 498, 520 ("limited" appearance of counsel in immigration proceedings prohibited by federal regulations); Cal. Rules of Court, Rules 5.70-5.71 repealed effective January 1, 2013, revised and renumbered as Rule 5.425 adopted effective January 1, 2013 (limited scope representation in family law cases); rule 3-400 (discussion).

THE STATE BAR OF CALIFORNIA
STANDING COMMITTEE ON
PROFESSIONAL RESPONSIBILITY AND CONDUCT
FORMAL OPINION NO. 2015-193

ISSUE: What are an attorney's ethical duties in the handling of discovery of electronically stored information?

DIGEST: An attorney's obligations under the ethical duty of competence evolve as new technologies develop and become integrated with the practice of law. Attorney competence related to litigation generally requires, among other things, and at a minimum, a basic understanding of, and facility with, issues relating to e-discovery, including the discovery of electronically stored information ("ESI"). On a case-by-case basis, the duty of competence may require a higher level of technical knowledge and ability, depending on the e-discovery issues involved in a matter, and the nature of the ESI. Competency may require even a highly experienced attorney to seek assistance in some litigation matters involving ESI. An attorney lacking the required competence for e-discovery issues has three options: (1) acquire sufficient learning and skill before performance is required; (2) associate with or consult technical consultants or competent counsel; or (3) decline the client representation. Lack of competence in e-discovery issues also may lead to an ethical violation of an attorney's duty of confidentiality.

AUTHORITIES INTERPRETED: Rules 3-100 and 3-110 of the Rules of Professional Conduct of the State Bar of California.[1/]

Business and Professions Code section 6068(e).

Evidence Code sections 952, 954 and 955.

STATEMENT OF FACTS

Attorney defends Client in litigation brought by Client's Chief Competitor in a judicial district that mandates consideration of e-discovery[2/] issues in its formal case management order, which is consistent with California Rules of Court, rule 3.728. Opposing Counsel demands e-discovery; Attorney refuses. They are unable to reach an agreement by the time of the initial case management conference. At that conference, an annoyed Judge informs both attorneys they have had ample prior notice that e-discovery would be addressed at the conference and tells them to return in two hours with a joint proposal.

In the ensuing meeting between the two lawyers, Opposing Counsel suggests a joint search of Client's network, using Opposing Counsel's chosen vendor, based upon a jointly agreed search term list. She offers a clawback agreement that would permit Client to claw back any inadvertently produced ESI that is protected by the attorney-client privilege and/or the work product doctrine ("Privileged ESI").

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

[2/] Electronically stored information ("ESI") is information that is stored in technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities (e.g., Code Civ. Proc., § 2016.020, sub. (d) – (e)). Electronic Discovery, also known as e-discovery, is the use of legal means to obtain ESI in the course of litigation for evidentiary purposes.

Attorney believes the clawback agreement will allow him to pull back anything he "inadvertently" produces. Attorney concludes that Opposing Counsel's proposal is acceptable and, after advising Client about the terms and obtaining Client's authority, agrees to Opposing Counsel's proposal. Judge thereafter approves the attorneys' joint agreement and incorporates it into a Case Management Order, including the provision for the clawback of Privileged ESI. The Court sets a deadline three months later for the network search to occur.

Back in his office, Attorney prepares a list of keywords he thinks would be relevant to the case, and provides them to Opposing Counsel as Client's agreed upon search terms. Attorney reviews Opposing Counsel's additional proposed search terms, which on their face appear to be neutral and not advantageous to one party or the other, and agrees that they may be included.

Attorney has represented Client before, and knows Client is a large company with an information technology ("IT") department. Client's CEO tells Attorney there is no electronic information it has not already provided to Attorney in hard copy form. Attorney assumes that the IT department understands network searches better than he does and, relying on that assumption and the information provided by CEO, concludes it is unnecessary to do anything further beyond instructing Client to provide Vendor direct access to its network on the agreed upon search date. Attorney takes no further action to review the available data or to instruct Client or its IT staff about the search or discovery. As directed by Attorney, Client gives Vendor unsupervised direct access to its network to run the search using the search terms.

Subsequently, Attorney receives an electronic copy of the data retrieved by Vendor's search and, busy with other matters, saves it in an electronic file without review. He believes that the data will match the hard copy documents provided by Client that he already has reviewed, based on Client's CEO's representation that all information has already been provided to Attorney.

A few weeks later, Attorney receives a letter from Opposing Counsel accusing Client of destroying evidence and/or spoliation. Opposing Counsel threatens motions for monetary and evidentiary sanctions. After Attorney receives this letter, he unsuccessfully attempts to open his electronic copy of the data retrieved by Vendor's search. Attorney hires an e-discovery expert ("Expert"), who accesses the data, conducts a forensic search, and tells Attorney potentially responsive ESI has been routinely deleted from Client's computers as part of Client's normal document retention policy, resulting in gaps in the document production. Expert also advises Attorney that, due to the breadth of Vendor's execution of the jointly agreed search terms, both privileged information and irrelevant but highly proprietary information about Client's upcoming revolutionary product were provided to Chief Competitor in the data retrieval. Expert advises Attorney that an IT professional with litigation experience likely would have recognized the overbreadth of the search and prevented the retrieval of the proprietary information.

What ethical issues face Attorney relating to the e-discovery issues in this hypothetical?

DISCUSSION

I. Duty of Competence

A. Did Attorney Violate The Duty of Competence Arising From His Own Acts/Omissions?

While e-discovery may be relatively new to the legal profession, an attorney's core ethical duty of competence remains constant. Rule 3-110(A) provides: "A member shall not intentionally, recklessly, or repeatedly fail to perform legal services with competence." Under subdivision (B) of that rule, "competence" in legal services shall mean to apply the diligence, learning and skill, and mental, emotional, and physical ability reasonably necessary for the performance of such service. Read together, a mere failure to act competently does not trigger discipline under rule 3-110. Rather, it is the failure to do so in a manner that is intentional, reckless or repeated that would result in a disciplinable rule 3-110 violation. (See *In the Matter of Torres* (Reviwe Dept. 2000) 4 Cal. State Bar Ct. Rptr. 138, 149 ("We have repeatedly held that negligent legal representation, even that amounting to legal malpractice, does not establish a [competence] rule 3-110(A) violation."); see also, *In the Matter of Gadda* (Review Dept. 2002) 4 Cal. State Bar Ct. Rptr. 416 (reckless and repeated acts); *In the Matter of Riordan* (Review Dept. 2007) 5 Cal. State Bar Ct. Rptr. 41 (reckless and repeated acts).)

Legal rules and procedures, when placed alongside ever-changing technology, produce professional challenges that attorneys must meet to remain competent. Maintaining learning and skill consistent with an attorney's duty of competence includes keeping "abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, . . ." ABA Model Rule 1.1, Comment [8].[3/] Rule 3-110(C) provides: "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." Another permissible choice would be to decline the representation. When e-discovery is at issue, association or consultation may be with a non-lawyer technical expert, if appropriate in the circumstances. Cal. State Bar Formal Opn. No. 2010-179.

Not every litigated case involves e-discovery. Yet, in today's technological world, almost every litigation matter *potentially* does. The chances are significant that a party or a witness has used email or other electronic communication, stores information digitally, and/or has other forms of ESI related to the dispute. The law governing e-discovery is still evolving. In 2009, the California Legislature passed California's Electronic Discovery Act adding or amending several California discovery statutes to make provisions for electronic discovery. See, e.g., Code of Civil Procedure section 2031.010, paragraph (a) (expressly providing for "copying, testing, or sampling" of "electronically stored information in the possession, custody, or control of any other party to the action.")[4/] However, there is little California case law interpreting the Electronic Discovery Act, and much of the development of e-discovery law continues to occur in the federal arena. Thus, to analyze a California attorney's current ethical obligations relating to e-discovery, we look to the federal jurisprudence for guidance, as well as applicable Model Rules, and apply those principles based upon California's ethical rules and existing discovery law.[5/]

We start with the premise that "competent" handling of e-discovery has many dimensions, depending upon the complexity of e-discovery in a particular case. The ethical duty of competence requires an attorney to assess at the outset of each case what electronic discovery issues might arise during the litigation, including the likelihood that e-discovery will or should be sought by either side. If e-discovery will probably be sought, the duty of competence requires an attorney to assess his or her own e-discovery skills and resources as part of the attorney's duty to provide the client with competent representation. If an attorney lacks such skills and/or resources, the attorney must try to acquire sufficient learning and skill, or associate or consult with someone with expertise to assist. Rule 3-110(C). Attorneys handling e-discovery should be able to perform (either by themselves or in association with competent co-counsel or expert consultants) the following:

- initially assess e-discovery needs and issues, if any;
- implement/cause to implement appropriate ESI preservation procedures;[6/]

[3/] Although not binding, opinions of ethics committees in California should be consulted by members for guidance on proper professional conduct. Ethics opinions and rules and standards promulgated by other jurisdictions and bar associations may also be considered. Rule 1-100(A).

[4/] In 2006, revisions were made to the Federal Rules of Civil Procedure, rules 16, 26, 33, 34, 37 and 45, to address e-discovery issues in federal litigation. California modeled its Electronic Discovery Act to conform with mostly-parallel provisions in those 2006 federal rules amendments. (See Evans, *Analysis of the Assembly Committee on Judiciary regarding AB 5* (2009). (http://www.leginfo.ca.gov/pub/09-10/bill/asm/ab_0001-0050/ab_5_cfa_20090302_114942_asm_comm.html).)

[5/] Federal decisions are compelling where the California law is based upon a federal statute or the federal rules. (See *Toshiba America Electronic Components, Inc. v. Superior Court (Lexar Media, Inc.)* (2004) 124 Cal.App.4th 762, 770 [21 Cal.Rptr.3d 532]*; Vasquez v. Cal. School of Culinary Arts, Inc.* (2014) 230 Cal.App.4th 35 [178 Cal.Rptr.3d 10]; see also footnote 4, *supra.*)

[6/] This opinion does not directly address ethical obligations relating to litigation holds. A litigation hold is a directive issued to, by, or on behalf of a client to persons or entities associated with the client who may possess potentially relevant documents (including ESI) that directs those custodians to preserve such documents, pending further direction. See generally Redgrave, *Sedona Conference ® Commentary on Legal Holds: The Trigger and The Process* (Fall 2010) The Sedona Conference Journal, Vol. 11 at pp. 260 – 270, 277 – 279. Prompt issuance of a litigation hold may prevent spoliation of evidence, and the duty to do so falls on both the party and outside counsel working on the matter. See

- analyze and understand a client's ESI systems and storage;
- advise the client on available options for collection and preservation of ESI;
- identify custodians of potentially relevant ESI;
- engage in competent and meaningful meet and confer with opposing counsel concerning an e-discovery plan;
- perform data searches;
- collect responsive ESI in a manner that preserves the integrity of that ESI; and
- produce responsive non-privileged ESI in a recognized and appropriate manner.[7/]

See, e.g., *Pension Committee of the University of Montreal Pension Plan v. Banc of America Securities, LLC* (S.D.N.Y. 2010) 685 F.Supp.2d 456, 462 – 465 (defining gross negligence in the preservation of ESI), (abrogated on other grounds in *Chin v. Port Authority* (2nd Cir. 2012) 685 F.3d 135 (failure to institute litigation hold did not constitute gross negligence per se)).

In our hypothetical, Attorney had a general obligation to make an e-discovery evaluation early, prior to the initial case management conference. The fact that it was the standard practice of the judicial district in which the case was pending to address e-discovery issues in formal case management highlighted Attorney's obligation to conduct an early initial e-discovery evaluation.

Notwithstanding this obligation, Attorney made *no* assessment of the case's e-discovery needs or of his own capabilities. Attorney exacerbated the situation by not consulting with another attorney or an e-discovery expert prior to agreeing to an e-discovery plan at the initial case management conference. He then allowed that proposal to become a court order, again with no expert consultation, although he lacked sufficient expertise. Attorney participated in preparing joint e-discovery search terms without experience or expert consultation, and he did not fully understand the danger of overbreadth in the agreed upon search terms.

Even after Attorney stipulated to a court order directing a search of Client's network, Attorney took no action other than to instruct Client to allow Vendor to have access to Client's network. Attorney did not instruct or supervise Client regarding the direct network search or discovery, nor did he try to pre-test the agreed upon search terms or otherwise review the data before the network search, relying on his assumption that Client's IT department would know what to do, and on the parties' clawback agreement.

After the search, busy with other matters and under the impression the data matched the hard copy documents he had already seen, Attorney took no action to review the gathered data until after Opposing Counsel asserted spoliation and threatened sanctions. Attorney then unsuccessfully attempted to review the search results. It was only then, at the end of this long line of events, that Attorney finally consulted an e-discovery expert and learned of the e-discovery problems facing Client. By this point, the potential prejudice facing Client was significant, and much of the damage already had been done.

At the least, Attorney risked breaching his duty of competence when he failed at the outset of the case to perform a timely e-discovery evaluation. Once Opposing Counsel insisted on the exchange of e-discovery, it became certain that e-discovery would be implicated, and the risk of a breach of the duty of competence grew considerably; this should have prompted Attorney to take additional steps to obtain competence, as contemplated under rule 3-110(C), such as consulting an e-discovery expert.

[Footnote Continued…]

Zubulake v. UBS Warburg LLC (S.D.N.Y. 2003) 220 F.R.D. 212, 218 and *Zubulake v. UBS Warburg LLC* (S.D.N.Y. 2004) 229 F.R.D. 422, 432. Spoliation of evidence can result in significant sanctions, including monetary and/or evidentiary sanctions, which may impact a client's case significantly.

[7/] This opinion focuses on an attorney's ethical obligations relating to his own client's ESI and, therefore, this list focuses on those issues. This opinion does not address the scope of an attorney's duty of competence relating to obtaining an opposing party's ESI.

Had the e-discovery expert been consulted at the beginning, or at the latest once Attorney realized e-discovery would be required, the expert could have taken various steps to protect Client's interest, including possibly helping to structure the search differently, or drafting search terms less likely to turn over privileged and/or irrelevant but highly proprietary material. An expert also could have assisted Attorney in his duty to counsel Client of the significant risks in allowing a third party unsupervised direct access to Client's system due to the high risks and how to mitigate those risks. An expert also could have supervised the data collection by Vendor.[8/]

Whether Attorney's acts/omissions in this single case amount to a disciplinable offense under the "intentionally, recklessly, or repeatedly" standard of rule 3-110 is beyond this opinion, yet such a finding could be implicated by these facts.[9/] See, e.g., *In the Matter of Respondent G.* (Review Dept. 1992) 2 Cal. State Bar Ct. Rptr. 175, 179 (respondent did not perform competently where he was reminded on repeated occasions of inheritance taxes owed and repeatedly failed to advise his clients of them); *In re Matter of Copren* (Review Dept. 2005) 4 Cal. State Bar Ct. Rptr. 861, 864 (respondent did not perform competently when he failed to take several acts in single bankruptcy matter); *In re Matter of Layton* (Review Dept. 1993) 2 Cal. State Bar Ct. Rptr. 366, 377 – 378 (respondent did not perform competently where he "recklessly" exceeded time to administer estate, failed to diligently sell/distribute real property, untimely settled supplemental accounting and did not notify beneficiaries of intentions not to sell/lease property).

B. Did Attorney Violate The Duty of Competence By Failing To Supervise?

The duty of competence in rule 3-110 includes the duty to supervise the work of subordinate attorneys and non-attorney employees or agents. See Discussion to rule 3-110. This duty to supervise can extend to outside vendors or contractors, and even to the client itself. See California State Bar Formal Opn. No. 2004-165 (duty to supervise outside contract lawyers); San Diego County Bar Association Formal Opn. No. 2012-1 (duty to supervise clients relating to ESI, citing *Cardenas v. Dorel Juvenile Group, Inc.* (D. Kan. 2006) 2006 WL 1537394).

Rule 3-110(C) permits an attorney to meet the duty of competence through association with another lawyer or consultation with an expert. See California State Bar Formal Opn. No. 2010-179. Such expert may be an outside vendor, a subordinate attorney, or even the client, if they possess the necessary expertise. This consultation or association, however, does not absolve an attorney's obligation to supervise the work of the expert under rule 3-110, which is a non-delegable duty belonging to the attorney who is counsel in the litigation, and who remains the one primarily answerable to the court. An attorney must maintain overall responsibility for the work of the expert he or she chooses, even if that expert is the client or someone employed by the client. The attorney must do so by remaining regularly engaged in the expert's work, by educating everyone involved in the e-discovery workup about the legal issues in the case, the factual matters impacting discovery, including witnesses and key evidentiary issues, the obligations around discovery imposed by the law or by the court, and of any relevant risks associated with the e-discovery tasks at hand. The attorney should issue appropriate instructions and guidance and, ultimately, conduct appropriate tests until satisfied that the attorney is meeting his ethical obligations prior to releasing ESI.

Here, relying on his familiarity with Client's IT department, Attorney assumed the department understood network searches better than he did. He gave them no further instructions other than to allow Vendor access on the date of the network search. He provided them with no information regarding how discovery works in litigation, differences

---

[8/] See Advisory Committee Notes to the 2006 Amendments to the Federal Rules of Civil Procedure, rule 34 ("Inspection or testing of certain types of electronically stored information or of a responding party's electronic information system may raise issues of confidentiality or privacy. The addition of testing and sampling to Rule 34(a) . . . is not meant to create a routine right of direct access to a party's electronic information system, although such access might be justified in some circumstances. Courts should guard against undue intrusiveness resulting from inspecting or testing such systems."). See also The Sedona Principles Addressing Electronic Document Production (2nd Ed. 2007), Comment 10(b) ("Special issues may arise with any request to secure direct access to electronically stored information or to computer devices or systems on which it resides. Protective orders should be in place to guard against any release of proprietary, confidential, or personal electronically stored information accessible to the adversary or its expert.").

[9/] This opinion does not intend to set or define a standard of care of attorneys for liability purposes, as standards of care can be highly dependent on the factual scenario and other factors not applicable to our analysis herein.

between a party affiliated vendor and a neutral vendor, what could constitute waiver under the law, what case-specific issues were involved, or the applicable search terms. Client allowed Vendor direct access to its entire network, without the presence of any Client representative to observe or monitor Vendor's actions. Vendor retrieved proprietary trade secret and privileged information, a result Expert advised Attorney could have been prevented had a trained IT individual been involved from the outset. In addition, Attorney failed to warn Client of the potential significant legal effect of not suspending its routine document deletion protocol under its document retention program.

Here, as with Attorney's own actions/inactions, whether Attorney's reliance on Client was reasonable and sufficient to satisfy the duty to supervise in this setting is a question for a trier of fact. Again, however, a potential finding of a competence violation is implicated by the fact pattern. See, e.g., *Palomo v. State Bar* (1984) 36 Cal.3d 785, 796 [205 Cal.Rptr. 834] (evidence demonstrated lawyer's pervasive carelessness in failing to give the office manager any supervision, or instruction on trust account requirements and procedures).

II. Duty of Confidentiality

A fundamental duty of an attorney is "[t]o maintain inviolate the confidence, and at every peril to himself or herself to preserve the secrets, of his or her client." (Bus. & Prof. Code, § 6068 (e)(1).) "Secrets" includes "information, other than that protected by the attorney-client privilege, that the client has requested be held inviolate or the disclosure of which would be embarrassing or would be likely to be detrimental to the client." (Cal. State Bar Formal Opinion No. 1988-96.) "A member shall not reveal information protected from disclosure by Business and Professions Code section 6068, subdivision (e)(1), without the informed consent of the client, or as provided in paragraph (B) of this rule." (Rule 3-100(A).)

Similarly, an attorney has a duty to assert the attorney-client privilege to protect confidential communications between the attorney and client. (Evid. Code, §§ 952, 954, 955.) In civil discovery, the attorney-client privilege will protect confidential communications between the attorney and client in cases of inadvertent disclosure *only if* the attorney and client act reasonably to protect that privilege. See *Regents of University of California v. Superior Court (Aquila Merchant Services, Inc.)* (2008) 165 Cal.App.4th 672, 683 [81 Cal.Rptr.3d 186]. This approach also echoes federal law. [10/] A lack of reasonable care to protect against disclosing privileged and protected information when producing ESI can be deemed a waiver of the attorney-client privilege. See *Kilopass Tech. Inc. v. Sidense Corp.* (N.D. Cal. 2012) 2012 WL 1534065 at 2 – 3 (attorney-client privilege deemed waived as to privileged documents released through e-discovery because screening procedures employed were unreasonable).

In our hypothetical, because of the actions taken by Attorney prior to consulting with any e-discovery expert, Client's privileged information has been disclosed. Due to Attorney's actions, Chief Competitor can argue that such disclosures were not "inadvertent" and that any privileges were waived. Further, non-privileged, but highly confidential proprietary information about Client's upcoming revolutionary new product has been released into the hands of Chief Competitor. Even absent any indication that Opposing Counsel did anything to engineer the overbroad disclosure, it remains true that the disclosure occurred because Attorney participated in creating overbroad search terms. All of this happened unbeknownst to Attorney, and only came to light after Chief Competitor accused Client of evidence spoliation. Absent Chief Competitor's accusation, it is not clear when any of this would have come to Attorney's attention, if ever.

The clawback agreement on which Attorney heavily relied may not work to retrieve the information from the other side. By its terms, the clawback agreement was limited to inadvertently produced Privileged ESI. Both privileged information, and non-privileged, but confidential and proprietary information, have been released to Chief Competitor.

[10/] See Federal Rules of Evidence, rule 502(b): "Inadvertent Disclosure. 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)."

Under these facts, Client may have to litigate whether Client (through Attorney) acted diligently enough to protect its attorney-client privileged communications. Attorney took no action to review Client's network prior to allowing the network search, did not instruct or supervise Client prior to or during Vendor's search, participated in drafting the overbroad search terms, and waited until after Client was accused of evidence spoliation before reviewing the data – all of which could permit Opposing Counsel viably to argue Client failed to exercise due care to protect the privilege, and the disclosure was not inadvertent.[11/]

Client also may have to litigate its right to the return of non-privileged but confidential proprietary information, which was not addressed in the clawback agreement.

Whether a waiver has occurred under these circumstances, and what Client's rights are to return of its non-privileged/confidential proprietary information, again are legal questions beyond this opinion. Attorney did not reasonably try to minimize the risks. Even if Client can retrieve the information, Client may never "un-ring the bell."

The State Bar Court Review Department has stated, "Section 6068, subdivision (e) is the most strongly worded duty binding on a California attorney. It requires the attorney to maintain 'inviolate' the confidence and 'at every peril to himself or herself' preserve the client's secrets." (See *Matter of Johnson* (Rev. Dept. 2000) 4 Cal. State Bar Ct. Rptr. 179.) While the law does not require perfection by attorneys in acting to protect privileged or confidential information, it requires the exercise of reasonable care. Cal. State Bar Formal Opn. No. 2010-179. Here, Attorney took only minimal steps to protect Client's ESI, or to instruct/supervise Client in the gathering and production of that ESI, and instead released everything without prior review, inappropriately relying on a clawback agreement. Client's secrets are now in Chief Competitor's hands, and further, Chief Competitor may claim that Client has waived the attorney-client privilege. Client has been exposed to that potential dispute as the direct result of Attorney's actions. Attorney may have breached his duty of confidentiality to Client.

CONCLUSION

Electronic document creation and/or storage, and electronic communications, have become commonplace in modern life, and discovery of ESI is now a frequent part of almost any litigated matter. Attorneys who handle litigation may not ignore the requirements and obligations of electronic discovery. Depending on the factual circumstances, a lack of technological knowledge in handling e-discovery may render an attorney ethically incompetent to handle certain litigation matters involving e-discovery, absent curative assistance under rule 3-110(C), even where the attorney may otherwise be highly experienced. It also may result in violations of the duty of confidentiality, notwithstanding a lack of bad faith conduct.

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 Trustees, any persons or tribunals charged with regulatory responsibilities, or any member of the State Bar.

*[**Publisher's Note**: Internet resources cited in this opinion were last accessed by staff on June 30, 2015. Copies of these resources are on file with the State Bar's Office of Professional Competence.]*

[11/] Although statute, rules, and/or case law provide some limited authority for the legal claw back of certain inadvertently produced materials, even in the absence of an express agreement, those provisions may not work to mitigate the damage caused by the production in this hypothetical. These "default" claw back provisions typically only apply to privilege and work product information, and require both that the disclosure at issue has been truly inadvertent, and that the holder of the privilege has taken reasonable steps to prevent disclosure in the first instance. See Federal Rules of Evidence, rule 502; see also generally *State Compensation Insurance Fund v. WPS, Inc.* (1999) 70 Cal.App.4th 644 [82 Cal.Rptr.2d 799]; *Rico v. Mitsubishi Motors Corp.* (2007) 42 Cal.4th 807, 817 – 818 [68 Cal.Rptr.3d 758]. As noted above, whether the disclosures at issue in our hypothetical truly were "inadvertent" under either the parties' agreement or the relevant law is an open question. Indeed, Attorney will find even less assistance from California's discovery clawback statute than he will from the federal equivalent, as the California statute merely addresses the procedure for litigating a dispute on a claim of inadvertent production, and not the legal issue of waiver at all. (See Code Civ. Proc., § 2031.285.)

THE STATE BAR OF CALIFORNIA
STANDING COMMITTEE ON
PROFESSIONAL RESPONSIBILITY AND CONDUCT
FORMAL OPINION INTERIM NO. 20-0004

ISSUES: What are a California lawyer's ethical duties when working remotely?

DIGEST: Remote practice does not alter a lawyer's ethical duties under the California Rules of Professional Conduct and the State Bar Act. Managerial lawyers must implement reasonable measures, policies, and practices to ensure continued compliance with these rules in a remote working environment, with a particular focus on the duties of confidentiality, technology competence, communication, and supervision.

AUTHORITIES INTERPRETED: Rules 1.1, 1.3, 1.4, 1.6, 5.1–5.3, and 5.5 of the Rules of Professional Conduct of the State Bar of California.[1]

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

Business and Professions Code sections 6125 et seq.

STATEMENT OF FACTS

A law firm ("Law Firm") decides that it would like to provide its lawyers and staff with the flexibility to work remotely and plans to move to a smaller, shared office space. Law Firm plans to implement a hybrid work environment to provide its lawyers and staff with the flexibility to work remotely and in the physical office when necessary. It plans to rent shared workspace for its new physical office. Law Firm wants to know what ethical obligations arise for Law Firm and its lawyers as a result of this anticipated transition to its working environment.

INTRODUCTION

In response to advances in technology, the California wildfires, the COVID-19 pandemic, and other circumstances, more and more lawyers are working remotely. The same rules of professional conduct that apply to attorneys practicing in traditional law firm offices apply to attorneys practicing remotely.[2] The application of the rules, however, raises unique issues for lawyers working remotely.[3] This opinion will focus on the primary rules that may be implicated by a lawyer's remote legal practice. While this opinion presents hypothetical facts to provide one common example, the ethical obligations discussed

[1] Unless otherwise indicated, all references to "rules" in this opinion will be to the Rules of Professional Conduct of the State Bar of California.

[2] See also, Cal. State Bar Formal Opn. No. 2012-184 (discussing lawyers' ethical obligations when practicing in a virtual law office).

[3] Many of these same issues are likewise implicated by lawyers who practice in virtual law offices. See, *id.*

herein would apply to lawyers who work remotely regardless of the underlying reasons or whether a traditional, physical office space remains available.

DISCUSSION

1. Duty of Confidentiality, Rule 1.6; Business and Professions Code Section 6068, Subdivision (e)

Because more lawyers and staff will be working remotely, Law Firm[4] needs to ensure that the technology it uses to facilitate remote practice is consistent with applicable ethical obligations, including the duty of confidentiality. Many of this committee's ethics opinions emphasize that lawyers must take reasonable measures to safeguard confidential client information when using technology to transmit and store confidential client information.[5] Law Firm may use third-party cloud providers to store or backup confidential client files or other technology solution vendors to facilitate remote practice. In doing so, Law Firm's managerial and supervisory lawyers must engage in reasonable efforts to ensure that these vendors' conduct is compatible with the lawyers' ethical obligations.[6] Reasonable measures include investigating the provider's reputation, history, security, and backup measures; limiting access to confidential information; carefully reviewing the terms of service to ensure that they contain adequate provisions concerning data security and the handling of breaches of confidentiality; and periodically reviewing and monitoring providers' policies, practices, and procedures to ensure that they remain compatible with the lawyers' ethical obligations.[7] If a lawyer is unable to evaluate the security of the technology used, the lawyer must seek additional information, or consult with someone who possesses the requisite knowledge to ensure compliance with the lawyer's duties of competence and confidentiality.[8]

When working from home, lawyers must implement reasonable measures to safeguard confidential client information, particularly if other household members share or have access to a home computer,

---

[4] Rule 1.0.1(c) defines a "law firm" as "a law partnership; a professional law corporation; a lawyer acting as a sole proprietorship; an association authorized to practice law; or lawyers employed in a legal services organization or in the legal department, division or office of a corporation, of a government organization, or of another organization." "Law Firm" is used in this opinion as shorthand in reference to the responsibilities of Law Firm's managerial lawyers. The rules regulate the conduct of lawyers, rather than law firms, through professional discipline. See, rule 1.0(a).

[5] See, e.g., Cal. State Bar Formal Opn. Nos. 2010-179 (addressing attorney's ethical duties of confidentiality and competence when using technology to transmit or store confidential client information); 2012-184 (addressing attorney's ethical obligation when practicing in a virtual law firms); 2015-193 (addressing attorney's ethical duties concerning e-discovery and referencing Comment [8] to ABA Model Rule 1.1); 2020-203 (addressing attorney's ethical obligations regarding data breaches); see also ABA Formal Ethics Opn. Nos. 477R (2017) and 483 (2018).

[6] Rule 5.3(a)–(b).

[7] For additional factors to consider in vetting and overseeing cloud providers, see Cal. State Bar Formal Opn. No. 2012-184 at pp. 3-4; Illinois State Bar Ass'n Professional Conduct Advisory Opn. 16-06; New York State Bar Ass'n Committee on Professional Ethics Opn. 842; and Pennsylvania Bar Ass'n Committee on Legal Ethics and Professional Responsibility Opn. 2011-200 at pp. 8-11. While beyond the scope of this ethics opinion, it would also be prudent for lawyers to consider applicable privacy laws, particularly if data are hosted outside of the United States. See ABA Model Rule 1.6, Cmt. [18]; Pennsylvania Bar Ass'n Committee on Legal Ethics and Professional Responsibility Opn. 2011-200 at p. 9.

[8] *Id*.

laptop, or printer.[9] Reasonable security measures might include creating separate accounts for household members, implementing two-factor authentication, strong passwords, and automatic logging off when the computer becomes inactive, and disabling the listening capability of smart speakers, virtual assistants, or other listening-enabled devices unless needed to assist with legal services.[10] To the extent physical files are used, lawyers must ensure that they are stored and disposed of securely. This opinion does not intend to set forth specific mandatory measures as technology and associated risks are continually evolving and the reasonableness of security measures will depend upon multiple factors, including the client's instructions or needs, the sensitivity of the information, the remote working environment (e.g., kitchen/dining room office or backyard), and the presence of third parties, such as household members, neighbors, and repair workers. The failure to implement reasonable security measures may jeopardize the duty of confidentiality or the attorney-client privilege.[11]

Because Law Firm will be moving to a smaller, shared office space, Law Firm will also need to implement reasonable measures to ensure that confidential client files (hard copy and electronic) are securely stored and not accessible by third parties sharing the office space. This committee and several bar associations have issued ethics opinions addressing lawyers' ethical obligations relating to shared office space, including protecting confidential client information, avoiding client confusion regarding the nature of the relationship among lawyers who share office space, and avoiding conflicts of interest.[12]

2. Duty of Competence, Rule 1.1

California recently amended rule 1.1 to incorporate a version of Comment [8] to ABA Model Rule 1.1, which is commonly referred to as a lawyer's "duty of technology competence."[13] Our prior ethics opinions also explain a lawyer's duty of technology competence.[14] The duty of technology competence applies to multiple aspects of a lawyer's practice, such as those involving electronic discovery, social media, law practice management, virtual law offices, and remote practice. The ABA Standing Committee on Ethics and Professional Responsibility declined to endorse strict rules relating to a lawyer's duty of technology competence but adopted a "reasonable efforts standard" and "fact-specific approach" based on the ABA Cybersecurity Handbook.[15] This committee agrees that this reasonableness standard applies to a lawyer's duty of technology competence.[16]

Law Firm must ensure that its technology solutions are sufficient to permit lawyers to reasonably access client files while working remotely. Requiring files to be saved to a centralized, secure case management

[9] This duty applies to other remote situations. See, Cal. State Bar Formal Opn. No. 2010-179.

[10] ABA Formal Ethics Opn. No. 498 (2021) at p. 6.

[11] See, e.g., Cal. State Bar Formal Opn. No. 2010-179 at p. 6; ABA Formal Ethics Opn. 498 at p. 5; ABA Formal Ethics Opn. 477R at p. 8.

[12] See, e.g., Cal. State Bar Formal Opn. No. 1997-150; Colorado Bar Ass'n Ethics Opn. No. 89 (revised and reissued on March 12, 2018); NYSBA Ethics Opn. No. 939 (2012); see also California Rule of Professional Conduct 7.1 and 7.5.

[13] Rule 1.1 (effective March 22, 2021), Cmt. [1] ("The duties set forth in this rule include the duty to keep abreast of the changes in the law and its practice, including the benefits and risks associated with relevant technology.").

[14] See Cal. State Bar Formal Opn. Nos. 2010-179; 2012-184; and 2015-193.

[15] ABA Formal Ethics Opn. No. 477R (2017) at p. 4.

[16] See, Cal. State Bar Formal Opn. Nos. 2020-203 at p. 5; 2010-179 at pp. 2–6.

system may help ensure reasonable access, for instance, if local files are lost or corrupted. Law Firm must also regularly back up files to ensure reasonable access in the event of data loss.[17]

Lawyers must also stay abreast of relevant court rules and procedures relating to COVID-19 and other disasters, including the closure or limited hours of courts, and be adequately prepared to render competent legal representation at remote court hearings and conferences.

In addition, a lawyer's duty of competence includes the "mental, emotional, and physical ability reasonably necessary for the performance" of legal services.[18] The health, personal (e.g., school closures, childcare, or other family responsibilities), or financial impacts of pandemics and other disasters may interfere with a lawyer's physical, mental, or emotional ability to competently perform legal services. Similarly, the remote working environment itself may also affect a lawyer's mental or emotional health.[19] The duty to render competent legal services is not generally excused under these circumstances.[20] Lawyers must take reasonable measures to ensure that they are able to provide competent legal services to their clients even in the event of a disaster. One way of doing so is to plan in advance to ensure that competent representation may still be rendered to clients in the event that a disaster adversely affects a lawyer's ability to render competent and diligent legal services.[21]

3. Duty of Communication, Rule 1.4

While working remotely, lawyers may increasingly communicate with prospective or current clients via a secure website portal, email, or other form of online communications, instead of in-person meetings. In communicating with prospective clients, Law Firm should take reasonable steps to avoid forming unintended attorney-client relationships, such as including disclaimers on its website or other online communications that posted information is not legal advice and that communication through the website does not create an attorney-client relationship. In addition, before entering into an engagement agreement, lawyers should obtain sufficient information from the client to screen for conflicts of interest and ensure that the party they are communicating with is the actual client or someone with authority to act on the client's behalf.[22]

Lawyers also need to ensure that any alternative means of communications with clients are adequate to fulfill their duty of communication. Among other requirements, a lawyer must "reasonably consult with

---

[17] ABA Formal Ethics Opn. No. 498 (2021) at p. 5.

[18] Rule 1.1(b)(ii).

[19] See, e.g., ABA Commission of Lawyers Assistance Program, January 2021 Update: https://www.americanbar.org/groups/lawyer_assistance/well-being-in-the-legal-profession/; California Lawyers Assistance Program: https://www.calbar.ca.gov/Attorneys/Attorney-Regulation/Lawyer-Assistance-Program; and Patrick Smith, *As Remote Work Brings Isolation, How Can Firms Keep Lawyers in the Fold?*: https://www.law.com/americanlawyer/2020/03/31/as-remote-work-brings-isolation-how-can-firms-keep-lawyers-in-the-fold/.

[20] *Smith v. State Bar* (1985) 38 Cal.3d 525, 540 [213 Cal.Rptr. 236] (decided under former rules).

[21] Rules 1.1 and 1.3; ABA Formal Ethics Opn. No. 482 ("Lawyers also must take reasonable steps in the event of a disaster to ensure access to funds the lawyer is holding in trust.").

[22] See, Cal. State Bar Formal Opn. No. 2012-184 at p. 5 (explaining that while lawyers in a traditional office environment have this same duty, the lack of in-person communication in connection with a virtual law office may make it more difficult for lawyers to make this determination, thus potentially requiring extra measures).

the client about the means by which to accomplish the client's objectives in the representation," and "keep the client reasonably informed about significant developments relating to the representation, including promptly complying with reasonable requests for information and copies of significant documents . . . ."[23] A lawyer must also "explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation."[24] When using electronic forms of communication, the lawyer must ensure that the client is receiving and understanding the information exchanged.[25] In certain circumstances, teleconferences or videoconferences may be needed. Even if litigation matters are delayed because of an emergency or another disaster, lawyers must continue to maintain communications with clients regarding the status of the case and any significant updates.[26]

Exchanging alternative contact information with clients will help ensure lawyer's continued ability to communicate with clients during an emergency.[27] Confirming schedules and availability with clients, which may be altered during an emergency, may help ensure that clients have sufficient time to review draft responses to discovery, pleadings, and other important documents relating to the representation.

If an emergency or illness adversely affects the lawyer's ability to represent clients, the lawyer must communicate with clients about the effect on the lawyer's representation to permit a client to make an informed decision regarding the representation.[28]

4. Duty of Supervision, Rules 5.1–5.3

California's rules relating to the duty of supervision reflect three separate sets of duties. First, rule 5.1 requires managerial and supervisory lawyers to make reasonable efforts to ensure compliance by other lawyers with the Rules of Professional Conduct and the State Bar Act. Second, a subordinate lawyer has an independent duty to comply with the rules and cannot simply follow the instruction of the lawyer's supervisor.[29] Third, lawyers responsible for managing non-lawyer staff are responsible for implementing reasonable steps to ensure that the conduct of non-lawyer staff, including independent contractors, is consistent with the lawyer's duties under the Rules of Professional Conduct.[30] In addition, lawyers with managerial authority in a law firm "shall make reasonable efforts to ensure that the firm has in effect

[23] Rule 1.4(a)(2)–(3).

[24] Rule 1.4(b).

[25] See, Cal. State Bar Formal Opn. No. 2012-184 at p. 5.

[26] See also rule 1.3(b) ("reasonable diligence" requires that "a lawyer acts with commitment and dedication to the interests of the client and does not neglect or disregard, or unduly delay a legal matter entrusted to the lawyer.").

[27] See, ABA Formal Ethics Opn. No. 482 at pp. 2–3 ("To be able to reach clients following a disaster, lawyers should maintain, or be able to create on short notice, electronic or paper lists of current clients and their contact information. This information should be stored in a manner that is easily accessible.").

[28] Rule 1.4(b); see also Oregon State Bar Coronavirus Response: Legal Ethics FAQ (2020) (providing detailed guidance on communications with clients relating to potential impacts of COVID-19 on representation, including manner of meetings, delay, assistance from another attorney, the continued ability to provide competent, diligent representation, and the potential need to withdraw).

[29] Rule 5.2.

[30] Rule 5.3(b), Comment.

measures giving reasonable assurance that the nonlawyer's conduct is compatible with the professional obligations of the lawyer."[31]

Under the facts presented, Law Firm must ensure that it provides appropriate tools and equipment, technology support, training, and monitoring to its lawyers and staff. Managerial lawyers could consult with appropriate information technology staff or consultants in implementing technology measures to assist with Law Firm's remote practice.

In addition, managerial lawyers at Law Firm must implement reasonable remote policies and practices, such as confidentiality and cybersecurity policies and training, to ensure the security of remote access and that the conduct of its lawyers and non-lawyers complies with the Rules of Professional Conduct. As an example, it is a good practice to carefully review the terms of any client guidelines for outside counsel, which may require specific confidentiality practices and cybersecurity insurance. To the extent Law Firm permits lawyers to use their own devices while working remotely, it is advisable for Law Firm to implement "Bring Your Own Device" (BYOD) policies that require lawyers and staff to maintain the confidentiality of firm and client data on personal devices.[32] Managerial lawyers are responsible for enforcing Law Firm's remote policies and procedures and regularly updating them to keep pace with advances in technology. In addition, all lawyers, including associates, who are working remotely must implement reasonable measures to comply with their professional duties while working remotely regardless of whether Law Firm has implemented any formal policies and procedures.[33]

Managerial lawyers and lawyers overseeing nonlawyers or other lawyers must maintain regular communications to oversee their work. Because Law Firm is maintaining a physical office, in-person trainings or meetings may assist in confirming that everyone is receiving and understanding the directions and guidance being provided. For law firms that decide to transition to "virtual only" environments, it is a good practice to use videoconferencing for important trainings or meetings.

Finally, as described above in connection with the duty of confidentiality, lawyers must adequately vet outside vendors and contractors and oversee their work to ensure it is consistent with the lawyer's ethical obligations. Written nondisclosure or confidentiality agreements may be appropriate for certain vendors as well as procedures to maintain reasonable access and control of client data.[34]

5. Unauthorized Practice of Law, Rule 5.5 and Business and Professions Code Sections 6125–6133

The committee recognizes that lawyers working remotely may temporarily or permanently relocate to another state where the lawyer is not licensed to practice law. This committee does not opine on issues of unauthorized practice of law, including whether a particular conduct or activity constitutes the

[31] Rule 5.3(a).

[32] For additional suggested BYOD practices, see ABA Formal Ethics Opn. No. 498 (2021) at p. 7. The Association of Corporate Counsel has also published resources for BYOD policies. See, e.g., Daniel B. Garrie, Senior Managing Partner, Law & Forensics LLC, *Top Ten Tips for Managing the "Bring Your Own Device to the Workplace" Environment*, available at: https://www.acc.com/resource-library/top-ten-tips-managing-bring-your-own-device-workplace-environment.

[33] See, rule 5.1(a) ("A lawyer shall comply with these rules and the State Bar Act notwithstanding that the lawyer acts at the direction of another lawyer or other person.").

[34] See, e.g., ABA Formal Ethics Opn. No. 498 (2021) at p. 7; Cal. State Bar Formal Opn. No. 2010-179 at pp. 4–5; New York State Bar Ass'n Ethics Opn. No. 842; Oregon State Bar Ethics Opn. No. 2011-188 (revised 2015).

unauthorized practice of law. California licensed lawyers practicing California law remotely in another state where they are not licensed should consult the multijurisdictional practice and unauthorized practice of law rules and authorities of the state where they are physically present.[35] The ABA and some other state bar and local ethics committees have issued opinions regarding unauthorized practice of law considerations for attorneys remotely practicing the law of the jurisdictions in which they are licensed while physically present in a jurisdiction in which they are not admitted.[36]

[35] See, rule 5.5(a)(1).

[36] See, e.g., ABA Formal Ethics Opn. No. 495 at pp. 3–4 ("[I]n the absence of a local jurisdiction's finding that the activity constitutes the unauthorized practice of law, a lawyer may practice the law authorized by the lawyer's licensing jurisdiction for clients of that jurisdiction, while physically located in a jurisdiction where the lawyer is not licensed if the lawyer does not hold out the lawyer's presence or availability to perform legal services in the local jurisdiction or actually provide legal services for matters subject to the local jurisdiction, unless otherwise authorized."); D.C. Court of Appeals Opn. No. 24-20 (2020) at p. 3 (concluding that the "incidental and temporary practice" exception under D.C. Court of Appeals Rule 49(c)(13) permitted an attorney who is not licensed in D.C. to practice law from their residence located in D.C., as long as the attorney "(1) is practicing from home due to the COVID-19 pandemic; (2) maintains a law office in a jurisdiction where the attorney is admitted to practice; (3) avoids using a D.C. address in any business document or otherwise holding out as authorized to practice law in D.C., and (4) does not regularly conduct in-person meetings with clients or third parties in D.C."); Delaware State Bar Ass'n Committee on Professional Ethics Opn. 2021-1 (concluding that "lawyers licensed in Delaware . . . may ethically engage in the practice of Delaware law, for clients with Delaware matters, while physically present in another jurisdiction in which they are not admitted" unless prohibited by the law of the other jurisdiction; lawyers may not hold themselves out as being licensed to practice in the other jurisdiction and may not advertise or otherwise hold themselves out as having an office in the other jurisdiction); Florida Bar Standing Committee on the Unlicensed Practice of Law Proposed Advisory Opn. No. FAO #2019-4, Out-of-State Attorney Working Remotely From Florida Home (2020) (approved by the Supreme Court of Florida on May 20, 2021) (finding that a New Jersey lawyer physically working from his home in Florida exclusively on federal intellectual property matters for his New Jersey law firm is not committing UPL in Florida as long as he does not hold himself or his firm out to the public as having a Florida presence, does not give advice about Florida law, and provides no legal services to Florida residents); New Jersey Committee on the Unauthorized Practice of Law Opn. 59 and Advisory Committee on Professional Ethics Opn. 742 (October 6, 2021) (non-New Jersey-licensed lawyers may practice out-of-state law from New Jersey, provided they do not maintain a "continuous and systematic presence" in New Jersey or hold themselves out as being available for the practice of law in New Jersey); Utah Ethics Advisory Committee Opn. No. 19-03 (2019) at p. 1 ("The Utah Rules of Professional Conduct do not prohibit an out-of-state attorney from representing clients from the state where the attorney is licensed even if the out-of-state attorney does so from his private location in Utah. However, in order to avoid engaging in the unauthorized practice of law, the out-of-state attorney who lives in Utah must not establish a public office in Utah or solicit Utah business."); Bar Ass'n of San Francisco Ethics Opn. 2021-1 ("A lawyer who is not licensed in California, and who does not advertise or otherwise hold himself or herself out as a licensed California lawyer, does not establish an office or other systematic or continuous presence for the practice of law in California, and does not represent a California person or entity, but is merely physically present in California while using modern technology to remotely practice law in compliance with the rules of the jurisdiction where the lawyer is licensed, should not be held in violation of California's Unauthorized Practice of Law ("UPL") rule and laws, specifically California Rules of Professional Conduct ("CRPC") Rule 5.5, or the State Bar Act, Business & Professions ("B&P") Code §§6125-6126.").

Lawyers not licensed in California who are working remotely in California should consult rule 5.5(b), California Rules of Court 9.40–9.48, Business and Professions Code sections 6125 et seq. and relevant authorities regarding multijurisdictional practice and the unauthorized practice of law.[37]

CONCLUSION

Lawyers may ethically practice remotely under the California Rules of Professional Conduct and the State Bar Act, provided they continue to comply with these rules, including the duties of confidentiality, competence, communication, and supervision. Lawyers must implement reasonable measures to ensure compliance that are tailored to the relevant circumstances and remote working environment.

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 Trustees, any persons, or tribunals charged with regulatory responsibilities, or any licensee of the State Bar.

*[**Publisher's Note:** Internet resources cited in this opinion were last accessed by staff on February 25, 2022. Copy of these resources are on file with the State Bar's Office of Professional Competence.]*

[37] See, *Birbrower, Montalbano, Condon & Frank, P.C. v. Sup. Ct.* (1998) 17 Cal.4th 119, 128–129 [70 Cal.Rptr.2d 304] (stating that "one may practice law in [California] in violation of section 6125 although not physically present here by advising a California client on California law in connection with a California legal dispute by telephone, fax, computer, or other modern technological means"); *In re Estate of Condon* (1998) 65 Cal.App.4th 1138, 1145–1146 [76 Cal.Rptr.2d 922] ("In the real world of 1998 we do not live or do business in isolation within strict geopolitical boundaries. Social interaction and the conduct of business transcends state and national boundaries; it is truly global. A tension is thus created between the right of a party to have counsel of his or her choice and the right of each geopolitical entity to control the activities of those who practice law within its borders.").

AMERICAN BAR ASSOCIATION

STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 483 **October 17, 2018**

Lawyers' Obligations After an Electronic Data Breach or Cyberattack

Model Rule 1.4 requires lawyers to keep clients "reasonably informed" about the status of a matter and to explain matters "to the extent reasonably necessary to permit a client to make an informed decision regarding the representation." Model Rules 1.1, 1.6, 5.1 and 5.3, as amended in 2012, address the risks that accompany the benefits of the use of technology by lawyers. When a data breach occurs involving, or having a substantial likelihood of involving, material client information, lawyers have a duty to notify clients of the breach and to take other reasonable steps consistent with their obligations under these Model Rules.

Introduction[1]

Data breaches and cyber threats involving or targeting lawyers and law firms are a major professional responsibility and liability threat facing the legal profession. As custodians of highly sensitive information, law firms are inviting targets for hackers.[2] In one highly publicized incident, hackers infiltrated the computer networks at some of the country's most well-known law firms, likely looking for confidential information to exploit through insider trading schemes.[3] Indeed, the data security threat is so high that law enforcement officials regularly divide business entities into two categories: those that have been hacked and those that will be.[4]

In Formal Opinion 477R, this Committee explained a lawyer's ethical responsibility to use reasonable efforts when communicating client confidential information using the Internet.[5] This

[1] This opinion is based on the ABA Model Rules of Professional Conduct as amended by the ABA House of Delegates through August 2018. The laws, court rules, regulations, rules of professional conduct and opinions promulgated in individual jurisdictions are controlling.

[2] *See, e.g.*, Dan Steiner, *Hackers Are Aggressively Targeting Law Firms' Data* (Aug. 3, 2017), https://www.cio.com (explaining that "[f]rom patent disputes to employment contracts, law firms have a lot of exposure to sensitive information. Because of their involvement, confidential information is stored on the enterprise systems that law firms use. . . . This makes them a juicy target for hackers that want to steal consumer information and corporate intelligence.")' *See also Criminal-Seeking-Hacker' Requests Network Breach for Insider Trading*, Private Industry Notification 160304-01, FBI, CYBER DIVISION (Mar. 4, 2016).

[3] Nicole Hong & Robin Sidel, *Hackers Breach Law Firms, Including Cravath and Weil Gotshal*, WALL ST. J. (Mar. 29, 2016), https://www.wsj.com/articles/hackers-breach-cravath-swaine-other-big-law-firms-1459293504.

[4] Robert S. Mueller, III, *Combatting Threats in the Cyber World Outsmarting Terrorists, Hackers and Spies*, FBI (Mar. 1, 2012), https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies.

[5] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R (2017) ("Securing Communication of Protected Client Information").

opinion picks up where Opinion 477R left off, and discusses an attorney's ethical obligations when a data breach exposes client confidential information. This opinion focuses on an attorney's ethical obligations after a data breach,[6] and it addresses only data breaches that involve information relating to the representation of a client. It does not address other laws that may impose post-breach obligations, such as privacy laws or other statutory schemes that law firm data breaches might also implicate. Each statutory scheme may have different post-breach obligations, including different notice triggers and different response obligations. Both the triggers and obligations in those statutory schemes may overlap with the ethical obligations discussed in this opinion. And, as a matter of best practices, attorneys who have experienced a data breach should review all potentially applicable legal response obligations. However, compliance with statutes such as state breach notification laws, HIPAA, or the Gramm-Leach-Bliley Act does not necessarily achieve compliance with ethics obligations. Nor does compliance with lawyer regulatory rules *per se* represent compliance with breach response laws. As a matter of best practices, lawyers who have suffered a data breach should analyze compliance separately under every applicable law or rule.

Compliance with the obligations imposed by the Model Rules of Professional Conduct, as set forth in this opinion, depends on the nature of the cyber incident, the ability of the attorney to know about the facts and circumstances surrounding the cyber incident, and the attorney's roles, level of authority, and responsibility in the law firm's operations.[7]

---

[6] The Committee recognizes that lawyers provide legal services to clients under a myriad of organizational structures and circumstances. The Model Rules of Professional Conduct refer to the various structures as a "firm." A "firm" is defined in Rule 1.0(c) as "a lawyer or lawyers in a law partnership, professional corporation, sole proprietorship or other association authorized to practice law; or lawyers employed in a legal services organization or the legal department of a corporation or other organization." How a lawyer complies with the obligations discussed in this opinion will vary depending on the size and structure of the firm in which a lawyer is providing client representation and the lawyer's position in the firm. *See* MODEL RULES OF PROF'L CONDUCT R. 5.1 (2018) (Responsibilities of Partners, Managers, and Supervisory Lawyers); MODEL RULES OF PROF'L CONDUCT R. 5.2 (2018) (Responsibility of a Subordinate Lawyers); and MODEL RULES OF PROF'L CONDUCT R. 5.3 (2018) (Responsibility Regarding Nonlawyer Assistance).

[7] In analyzing how to implement the professional responsibility obligations set forth in this opinion, lawyers may wish to consider obtaining technical advice from cyber experts. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R (2017) ("Any lack of individual competence by a lawyer to evaluate and employ safeguards to protect client confidences may be addressed through association with another lawyer or expert, or by education.") *See also, e.g.*, *Cybersecurity Resources*, ABA Task Force on Cybersecurity, https://www.americanbar.org/groups/cybersecurity/resources.html (last visited Oct. 5, 2018).

I. Analysis

A. Duty of Competence

Model Rule 1.1 requires that "A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."[8] The scope of this requirement was clarified in 2012, when the ABA recognized the increasing impact of technology on the practice of law and the obligation of lawyers to develop an understanding of that technology. Comment [8] to Rule 1.1 was modified in 2012 to read:

> To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology*, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject. (Emphasis added.)[9]

In recommending the change to Rule 1.1's Comment, the ABA Commission on Ethics 20/20 explained:

> Model Rule 1.1 requires a lawyer to provide competent representation, and Comment [6] [renumbered as Comment [8]] specifies that, to remain competent, lawyers need to 'keep abreast of changes in the law and its practice.' The Commission concluded that, in order to keep abreast of changes in law practice in a digital age, lawyers necessarily need to understand basic features of relevant technology and that this aspect of competence should be expressed in the Comment. For example, a lawyer would have difficulty providing competent legal services in today's environment without knowing how to use email or create an electronic document. [10]

---

[8] MODEL RULES OF PROF'L CONDUCT R. 1.1 (2018).

[9] A LEGISLATIVE HISTORY: THE DEVELOPMENT OF THE ABA MODEL RULES OF PROFESSIONAL CONDUCT, 1982-2013, at 43 (Art Garwin ed., 2013).

[10] ABA COMMISSION ON ETHICS 20/20 REPORT 105A (Aug. 2012), http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120808_revised_resolution_105a_as_amended.authcheckdam.pdf. The 20/20 Commission also noted that modification of Comment [6] did not change the lawyer's substantive duty of competence: "Comment [6] already encompasses an obligation to remain aware of changes in technology that affect law practice, but the Commission concluded that making this explicit, by addition of the phrase 'including the benefits and risks associated with relevant technology,' would offer greater clarity in this area and emphasize the importance of technology to modern law practice. The proposed amendment, which appears in a Comment, does not impose any new obligations on lawyers. Rather, the amendment is intended to serve as a reminder to lawyers that they should remain aware of technology, including the benefits and risks associated with it, as part of a lawyer's general ethical duty to remain competent."

In the context of a lawyer's post-breach responsibilities, both Comment [8] to Rule 1.1 and the 20/20 Commission's thinking behind it require lawyers to understand technologies that are being used to deliver legal services to their clients. Once those technologies are understood, a competent lawyer must use and maintain those technologies in a manner that will reasonably safeguard property and information that has been entrusted to the lawyer. A lawyer's competency in this regard may be satisfied either through the lawyer's own study and investigation or by employing or retaining qualified lawyer and nonlawyer assistants.[11]

1. Obligation to Monitor for a Data Breach

Not every cyber episode experienced by a lawyer is a data breach that triggers the obligations described in this opinion. A data breach for the purposes of this opinion means a data event where material client confidential information is misappropriated, destroyed or otherwise compromised, or where a lawyer's ability to perform the legal services for which the lawyer is hired is significantly impaired by the episode.

Many cyber events occur daily in lawyers' offices, but they are not a data breach because they do not result in actual compromise of material client confidential information. Other episodes rise to the level of a data breach, either through exfiltration/theft of client confidential information or through ransomware, where no client information is actually accessed or lost, but where the information is blocked and rendered inaccessible until a ransom is paid. Still other compromises involve an attack on a lawyer's systems, destroying the lawyer's infrastructure on which confidential information resides and incapacitating the attorney's ability to use that infrastructure to perform legal services.

Model Rules 5.1 and 5.3 impose upon lawyers the obligation to ensure that the firm has in effect measures giving reasonable assurance that all lawyers and staff in the firm conform to the Rules of Professional Conduct. Model Rule 5.1 Comment [2], and Model Rule 5.3 Comment [1] state that lawyers with managerial authority within a firm must make reasonable efforts to establish

[11] MODEL RULES OF PROF'L CONDUCT R. 5.3 (2018); ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R (2017); ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 08-451 (2018); *See also* JILL D. RHODES & ROBERT S. LITT, THE ABA CYBERSECURITY HANDBOOK: A RESOURCE FOR ATTORNEYS, LAW FIRMS, AND BUSINESS PROFESSIONALS 124 (2d ed. 2018) [hereinafter ABA CYBERSECURITY HANDBOOK].

internal policies and procedures designed to provide reasonable assurance that all lawyers and staff in the firm will conform to the Rules of Professional Conduct. Model Rule 5.1 Comment [2] further states that "such policies and procedures include those designed to detect and resolve conflicts of interest, identify dates by which actions must be taken in pending matters, account for client funds and property and ensure that inexperienced lawyers are properly supervised."

Applying this reasoning, and based on lawyers' obligations (i) to use technology competently to safeguard confidential information against unauthorized access or loss, and (ii) to supervise lawyers and staff, the Committee concludes that lawyers must employ reasonable efforts to monitor the technology and office resources connected to the internet, external data sources, and external vendors providing services relating to data[12] and the use of data. Without such a requirement, a lawyer's recognition of any data breach could be relegated to happenstance --- and the lawyer might not identify whether a breach has occurred,[13] whether further action is warranted,[14] whether employees are adhering to the law firm's cybersecurity policies and procedures so that the lawyers and the firm are in compliance with their ethical duties,[15] and how and when the lawyer must take further action under other regulatory and legal provisions.[16] Thus, just as lawyers must safeguard and monitor the security of paper files and actual client property, lawyers utilizing technology have the same obligation to safeguard and monitor the security of electronically stored client property and information.[17]

While lawyers must make reasonable efforts to monitor their technology resources to detect a breach, an ethical violation does not necessarily occur if a cyber-intrusion or loss of electronic information is not immediately detected, because cyber criminals might successfully hide their

[12] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 08-451 (2008).
[13] Fredric Greene, *Cybersecurity Detective Controls—Monitoring to Identify and Respond to Threats*, ISACA J., Vol. 5, 1025 (2015), *available at* https://www.isaca.org/Journal/archives/2015/Volume-5/Pages/cybersecurity-detective-controls.aspx (noting that "[d]etective controls are a key component of a cybersecurity program in providing visibility into malicious activity, breaches and attacks on an organization's IT environment.").
[14] MODEL RULES OF PROF'L CONDUCT R. 1.6(c) (2018); MODEL RULES OF PROF'L CONDUCT R. 1.15 (2018).
[15] *See also* MODEL RULES OF PROF'L CONDUCT R. 5.1 & 5.3 (2018).
[16] The importance of monitoring to successful cybersecurity efforts is so critical that in 2015, Congress passed the Cybersecurity Information Sharing Act of 2015 (CISA) to authorize companies to monitor and implement defensive measures on their information systems, and to foreclose liability for such monitoring under CISA. AUTOMATED INDICATOR SHARING, https://www.us-cert.gov/ais (last visited Oct. 5, 2018); *See also* National Cyber Security Centre "Ten Steps to Cyber Security" [Step 8: Monitoring] (Aug. 9, 2016), https://www.ncsc.gov.uk/guidance/10-steps-cyber-security.
[17] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R (2017).

intrusion despite reasonable or even extraordinary efforts by the lawyer. Thus, as is more fully explained below, the potential for an ethical violation occurs when a lawyer does not undertake reasonable efforts to avoid data loss or to detect cyber-intrusion, and that lack of reasonable effort is the cause of the breach.

2. Stopping the Breach and Restoring Systems

When a breach of protected client information is either suspected or detected, Rule 1.1 requires that the lawyer act reasonably and promptly to stop the breach and mitigate damage resulting from the breach. How a lawyer does so in any particular circumstance is beyond the scope of this opinion. As a matter of preparation and best practices, however, lawyers should consider proactively developing an incident response plan with specific plans and procedures for responding to a data breach.[18] The decision whether to adopt a plan, the content of any plan, and actions taken to train and prepare for implementation of the plan, should be made before a lawyer is swept up in an actual breach. "One of the benefits of having an incident response capability is that it supports responding to incidents systematically (i.e., following a consistent incident handling methodology) so that the appropriate actions are taken. Incident response plans help personnel to minimize loss or theft of information and disruption of services caused by incidents."[19] While every lawyer's response plan should be tailored to the lawyer's or the law firm's specific practice, as a general matter incident response plans share common features:

> The primary goal of any incident response plan is to have a process in place that will allow the firm to promptly respond in a coordinated manner to any type of security incident or cyber intrusion. The incident response process should promptly: identify and evaluate any potential network anomaly or intrusion; assess its nature and scope; determine if any data or information may have been accessed or compromised; quarantine the threat or malware; prevent the exfiltration of information from the firm; eradicate the malware, and restore the integrity of the firm's network.
>
> Incident response plans should identify the team members and their backups; provide the means to reach team members at any time an intrusion is reported, and

[18] *See* ABA CYBERSECURITY HANDBOOK, *supra* note 11, at 202 (explaining the utility of large law firms adopting "an incident response plan that details who has ownership of key decisions and the process to follow in the event of an incident.").

[19] *NIST Computer Security Incident Handling Guide*, at 6 (2012), https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf.

> define the roles of each team member. The plan should outline the steps to be taken at each stage of the process, designate the team member(s) responsible for each of those steps, as well as the team member charged with overall responsibility for the response.[20]

Whether or not the lawyer impacted by a data breach has an incident response plan in place, after taking prompt action to stop the breach, a competent lawyer must make all reasonable efforts to restore computer operations to be able again to service the needs of the lawyer's clients. The lawyer may do so either on her own, if qualified, or through association with experts. This restoration process provides the lawyer with an opportunity to evaluate what occurred and how to prevent a reoccurrence consistent with the obligation under Model Rule 1.6(c) that lawyers "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of the client."[21] These reasonable efforts could include (i) restoring the technology systems as practical, (ii) the implementation of new technology or new systems, or (iii) the use of no technology at all if the task does not require it, depending on the circumstances.

3. Determining What Occurred

The Model Rules do not impose greater or different obligations on a lawyer as a result of a breach involving client information, regardless of whether the breach occurs through electronic or physical means. Just as a lawyer would need to assess which paper files were stolen from the lawyer's office, so too lawyers must make reasonable attempts to determine whether electronic files were accessed, and if so, which ones. A competent attorney must make reasonable efforts to determine what occurred during the data breach. A post-breach investigation requires that the lawyer gather sufficient information to ensure the intrusion has been stopped and then, to the extent reasonably possible, evaluate the data lost or accessed. The information gathered in a post-breach investigation is necessary to understand the scope of the intrusion and to allow for accurate disclosure to the client consistent with the lawyer's duty of communication and honesty under

[20] Steven M. Puiszis, *Prevention and Response: A Two-Pronged Approach to Cyber Security and Incident Response Planning*, THE PROF'L LAWYER, Vol. 24, No. 3 (Nov. 2017).
[21] We discuss Model Rule 1.6(c) further below. But in restoring computer operations, lawyers should consider whether the lawyer's computer systems need to be upgraded or otherwise modified to address vulnerabilities, and further, whether some information is too sensitive to continue to be stored electronically.

Model Rules 1.4 and 8.4(c).[22] Again, how a lawyer actually makes this determination is beyond the scope of this opinion. Such protocols may be a part of an incident response plan.

B. Duty of Confidentiality

In 2012, amendments to Rule 1.6 modified both the Rule and the commentary about a lawyer's efforts that are required to preserve the confidentiality of information relating to the representation of a client. Model Rule 1.6(a) requires that "A lawyer shall not reveal information relating to the representation of a client" unless certain circumstances arise.[23] The 2012 modification added a duty in paragraph (c) that: "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."[24]

Amended Comment [18] explains:

> Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and 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. 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.

Recognizing the necessity of employing a fact-based analysis, Comment [18] to Model Rule 1.6(c) includes nonexclusive factors to guide lawyers in making a "reasonable efforts" determination. Those factors include:

- 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

---

[22] The rules against dishonesty and deceit may apply, for example, where the lawyer's failure to make an adequate disclosure --- or any disclosure at all --- amounts to deceit by silence. *See, e.g.*, MODEL RULES OF PROF'L CONDUCT R. 4.1 cmt. [1] (2018) ("Misrepresentations can also occur by partially true but misleading statements or omissions that are the equivalent of affirmative false statements.").

[23] MODEL RULES OF PROF'L CONDUCT R. 1.6(a) (2018).

[24] *Id.* at (c).

- 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).[25]

As this Committee recognized in ABA Formal Opinion 477R:

> At the intersection of a lawyer's competence obligation to keep "abreast of knowledge of the benefits and risks associated with relevant technology," and confidentiality obligation to make "reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client," lawyers must exercise reasonable efforts when using technology in communicating about client matters. What constitutes reasonable efforts is not susceptible to a hard and fast rule, but rather is contingent upon a set of factors.

As discussed above and in Formal Opinion 477R, an attorney's competence in preserving a client's confidentiality is not a strict liability standard and does not require the lawyer to be invulnerable or impenetrable.[26] Rather, the obligation is one of reasonable efforts. Rule 1.6 is not violated even if data is lost or accessed if the lawyer has made reasonable efforts to prevent the loss or access.[27] As noted above, this obligation includes efforts to monitor for breaches of client confidentiality. The nature and scope of this standard is addressed in the ABA Cybersecurity Handbook:

> Although security is relative, a legal standard for "reasonable" security is emerging. That standard rejects requirements for specific security measures (such as firewalls, passwords, or the like) and instead adopts 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 the measures are effectively implemented, and ensure that they are continually updated in response to new developments.[28]

---

[25] MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. [18] (2018). "The [Ethics 20/20] Commission examined the possibility of offering more detailed guidance about the measures that lawyers should employ. The Commission concluded, however, that technology is changing too rapidly to offer such guidance and that the particular measures lawyers should use will necessarily change as technology evolves and as new risks emerge and new security procedures become available." ABA COMMISSION REPORT 105A, *supra* note 9, at 5.

[26] ABA CYBERSECURITY HANDBOOK, *supra* note 11, at 122.

[27] MODEL RULES OF PROF'L CONDUCT R. 1.6, cmt. [18] (2018) ("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.")

[28] ABA CYBERSECURITY HANDBOOK, *supra* note 11, at 73.

Finally, Model Rule 1.6 permits a lawyer to reveal information relating to the representation of a client if the disclosure is impliedly authorized in order to carry out the representation. Such disclosures are permitted if the lawyer reasonably believes that disclosure: (1) is impliedly authorized and will advance the interests of the client in the representation, and (2) will not affect a material interest of the client adversely.[29] In exercising this discretion to disclose information to law enforcement about the data breach, the lawyer must consider: (i) whether the client would object to the disclosure; (ii) whether the client would be harmed by the disclosure; and (iii) whether reporting the theft would benefit the client by assisting in ending the breach or recovering stolen information. Even then, without consent, the lawyer may disclose only such information as is reasonably necessary to assist in stopping the breach or recovering the stolen information.

C. Lawyer's Obligations to Provide Notice of Data Breach

When a lawyer knows or reasonably should know a data breach has occurred, the lawyer must evaluate notice obligations. Due to record retention requirements of Model Rule 1.15, information compromised by the data breach may belong or relate to the representation of a current client or former client.[30] We address each below.

1. Current Client

Communications between a lawyer and current client are addressed generally in Model Rule 1.4. Rule 1.4(a)(3) provides that a lawyer must "keep the client reasonably informed about the status of the matter." Rule 1.4(b) provides: "A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation." Under these provisions, an obligation exists for a lawyer to communicate with current clients about a data breach.[31]

---

[29] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 01-421(2001) (disclosures to insurer in bills when lawyer representing insured).

[30] This opinion addresses only obligations to clients and former clients. Data breach, as used in this opinion, is limited to client confidential information. We do not address ethical duties, if any, to third parties.

[31] Relying on Rule 1.4 generally, the New York State Bar Committee on Professional Ethics concluded that a lawyer must notify affected clients of information lost through an online data storage provider. N.Y. State Bar Ass'n Op. 842 (2010) (Question 10: "If the lawyer learns of any breach of confidentiality by the online storage provider, then the lawyer must investigate whether there has been any breach of his or her own clients' confidential information,

Our conclusion here is consistent with ABA Formal Ethics Opinion 95-398 where this Committee said that notice must be given to clients if a breach of confidentiality was committed by or through a third-party computer vendor or other service provider. There, the Committee concluded notice to the client of the breach may be required under 1.4(b) for a "serious breach."[32] The Committee advised:

> Where the unauthorized release of confidential information could reasonably be viewed as a significant factor in the representation, for example where it is likely to affect the position of the client or the outcome of the client's legal matter, disclosure of the breach would be required under Rule 1.4(b).[33]

A data breach under this opinion involves the misappropriation, destruction or compromise of client confidential information, or a situation where a lawyer's ability to perform the legal services for which the lawyer was hired is significantly impaired by the event. Each of these scenarios is one where a client's interests have a reasonable possibility of being negatively impacted. When a data breach occurs involving, or having a substantial likelihood of involving, material client confidential information a lawyer has a duty to notify the client of the breach. As noted in ABA Formal Opinion 95-398, a data breach requires notice to the client because such notice is an integral part of keeping a "client reasonably informed about the status of the matter" and the lawyer should provide information as would be "reasonably necessary to permit the client to make informed decisions regarding the representation" within the meaning of Model Rule 1.4.[34]

The strong client protections mandated by Model Rule 1.1, 1.6, 5.1 and 5.3, particularly as they were amended in 2012 to account for risks associated with the use of technology, would be compromised if a lawyer who experiences a data breach that impacts client confidential information is permitted to hide those events from their clients. And in view of the duties imposed by these other Model Rules, Model Rule 1.4's requirement to keep clients "reasonably informed about the status" of a matter would ring hollow if a data breach was somehow excepted from this responsibility to communicate.

---

notify any affected clients, and discontinue use of the service unless the lawyer receives assurances that any security issues have been sufficiently remediated.") (*citations omitted*).

[32] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 95-398 (1995).

[33] *Id.*

[34] MODEL RULES OF PROF'L CONDUCT R. 1.4(b) (2018).

Model Rule 1.15(a) provides that a lawyer shall hold "property" of clients "in connection with a representation separate from the lawyer's own property." Funds must be kept in a separate account, and "[o]ther property shall be identified as such and appropriately safeguarded." Model Rule 1.15(a) also provides that, "Complete records of such account funds and other property shall be kept by the lawyer . . . ." Comment [1] to Model Rule 1.15 states:

> A lawyer should hold property of others with the care required of a professional fiduciary. Securities should be kept in a safe deposit box, except when some other form of safekeeping is warranted by special circumstances. All property that is the property of clients or third persons, including prospective clients, must be kept separate from the lawyer's business and personal property.

An open question exists whether Model Rule 1.15's reference to "property" includes information stored in electronic form. Comment [1] uses as examples "securities" and "property" that should be kept separate from the lawyer's "business and personal property." That language suggests Rule 1.15 is limited to tangible property which can be physically segregated. On the other hand, many courts have moved to electronic filing and law firms routinely use email and electronic document formats to image or transfer information. Reading Rule 1.15's safeguarding obligation to apply to hard copy client files but not electronic client files is not a reasonable reading of the Rule.

Jurisdictions that have addressed the issue are in agreement. For example, Arizona Ethics Opinion 07-02 concluded that client files may be maintained in electronic form, with client consent, but that lawyers must take reasonable precautions to safeguard the data under the duty imposed in Rule 1.15. The District of Columbia Formal Ethics Opinion 357 concluded that, "Lawyers who maintain client records solely in electronic form should take reasonable steps (1) to ensure the continued availability of the electronic records in an accessible form during the period for which they must be retained and (2) to guard against the risk of unauthorized disclosure of client information."

The Committee has engaged in considerable discussion over whether Model Rule 1.15 and, taken together, the technology amendments to Rules 1.1, 1.6, and 5.3 impliedly impose an obligation on a lawyer to notify a current client of a data breach. We do not have to decide that question in the absence of concrete facts. We reiterate, however, the obligation to inform the client does exist under Model Rule 1.4.

2. Former Client

Model Rule 1.9(c) requires that "A lawyer who has formerly represented a client in a matter or whose present or former firm has formerly represented a client in a matter shall not thereafter . . . reveal information relating to the representation except as these Rules would permit or require with respect to a client."[35] When electronic "information relating to the representation" of a former client is subject to unauthorized access, disclosure, or destruction, the Model Rules provide no direct guidance on a lawyer's obligation to notify the former client. Rule 1.9(c) provides that a lawyer "shall not . . . reveal" the former client's information. It does not describe what steps, if any, a lawyer should take if such information is revealed. The Committee is unwilling to require notice to a former client as a matter of legal ethics in the absence of a black letter provision requiring such notice.[36]

Nevertheless, we note that clients can make an informed waiver of the protections in Rule 1.9.[37] We also note that Rule 1.16(d) directs that lawyers should return "papers and property" to clients at the conclusion of the representation, which has commonly been understood to include the client's file, in whatever form it is held. Rule 1.16(d) also has been interpreted as permitting lawyers to establish appropriate data destruction policies to avoid retaining client files and property indefinitely.[38] Therefore, as a matter of best practices, lawyers are encouraged to reach agreement with clients before conclusion, or at the termination, of the relationship about how to handle the client's electronic information that is in the lawyer's possession.

Absent an agreement with the former client lawyers are encouraged to adopt and follow a paper and electronic document retention schedule, which meets all applicable laws and rules, to reduce the amount of information relating to the representation of former clients that the lawyers retain. In addition, lawyers should recognize that in the event of a data breach involving former client information, data privacy laws, common law duties of care, or contractual arrangements with

---

[35] MODEL RULES OF PROF'L CONDUCT R. 1.9(c)(2) (2018).
[36] *See* Discipline of Feland, 2012 ND 174, ¶ 19, 820 N.W.2d 672 (Rejecting respondent's argument that the court should engraft an additional element of proof in a disciplinary charge because "such a result would go beyond the clear language of the rule and constitute amendatory rulemaking within an ongoing disciplinary proceeding.").
[37] *See* MODEL RULES OF PROF'L CONDUCT R. 1.9, cmt. [9] (2018).
[38] *See* ABA Ethics Search Materials on Client File Retention, https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/piles_of_files_2008.pdf (last visited Oct.15, 2018).

the former client relating to records retention, may mandate notice to former clients of a data breach. A prudent lawyer will consider such issues in evaluating the response to the data breach in relation to former clients.[39]

3. Breach Notification Requirements

The nature and extent of the lawyer's communication will depend on the type of breach that occurs and the nature of the data compromised by the breach. Unlike the "safe harbor" provisions of Comment [18] to Model Rule 1.6, if a post-breach obligation to notify is triggered, a lawyer must make the disclosure irrespective of what type of security efforts were implemented prior to the breach. For example, no notification is required if the lawyer's office file server was subject to a ransomware attack but no information relating to the representation of a client was inaccessible for any material amount of time, or was not accessed by or disclosed to unauthorized persons. Conversely, disclosure will be required if material client information was actually or reasonably suspected to have been accessed, disclosed or lost in a breach.

The disclosure must be sufficient to provide enough information for the client to make an informed decision as to what to do next, if anything. In a data breach scenario, the minimum disclosure required to all affected clients under Rule 1.4 is that there has been unauthorized access to or disclosure of their information, or that unauthorized access or disclosure is reasonably suspected of having occurred. Lawyers must advise clients of the known or reasonably ascertainable extent to which client information was accessed or disclosed. If the lawyer has made reasonable efforts to ascertain the extent of information affected by the breach but cannot do so, the client must be advised of that fact.

In addition, and as a matter of best practices, a lawyer also should inform the client of the lawyer's plan to respond to the data breach, from efforts to recover information (if feasible) to steps being taken to increase data security.

The Committee concludes that lawyers have a continuing duty to keep clients reasonably apprised of material developments in post-breach investigations affecting the clients'

[39] *Cf.* ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 482 (2018), at 8-10 (discussing obligations regarding client files lost or destroyed during disasters like hurricanes, floods, tornadoes, and fires).

information.[40] Again, specific advice on the nature and extent of follow up communications cannot be provided in this opinion due to the infinite number of variable scenarios.

If personally identifiable information of clients or others is compromised as a result of a data beach, the lawyer should evaluate the lawyer's obligations under state and federal law. All fifty states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have statutory breach notification laws.[41] Those statutes require that private or governmental entities notify individuals of breaches involving loss or disclosure of personally identifiable information.[42] Most breach notification laws specify who must comply with the law, define "personal information," define what constitutes a breach, and provide requirements for notice.[43] Many federal and state agencies also have confidentiality and breach notification requirements.[44] These regulatory schemes have the potential to cover individuals who meet particular statutory notice triggers, irrespective of the individual's relationship with the lawyer. Thus, beyond a Rule 1.4 obligation, lawyers should evaluate whether they must provide a statutory or regulatory data breach notification to clients or others based upon the nature of the information in the lawyer's possession that was accessed by an unauthorized user.[45]

III. Conclusion

Even lawyers who, (i) under Model Rule 1.6(c), make "reasonable efforts to prevent the . . . unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client," (ii) under Model Rule 1.1, stay abreast of changes in technology, and (iii) under Model Rules 5.1 and 5.3, properly supervise other lawyers and third-party electronic-information storage vendors, may suffer a data breach. When they do, they have a duty to notify clients of the data

[40] State Bar of Mich. Op. RI-09 (1991).
[41] National Conference of State Legislatures, *Security Breach Notification Laws* (Sept. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.
[42] *Id.*
[43] *Id.*
[44] ABA CYBERSECURITY HANDBOOK, *supra* note 11, at 65.
[45] Given the broad scope of statutory duties to notify, lawyers would be well served to actively manage the amount of confidential and or personally identifiable information they store beyond any ethical, statutory, or other legal obligation to do so. Lawyers should implement, and follow, a document retention policy that comports with Model Rule 1.15 and evaluate ways to limit receipt, possession and/or retention of confidential or personally identifiable information during or after an engagement.

breach under Model Rule 1.4 in sufficient detail to keep clients "reasonably informed" and with an explanation "to the extent necessary to permit the client to make informed decisions regarding the representation."

AMERICAN BAR ASSOCIATION

STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 495 **December 16, 2020**

Lawyers Working Remotely

Lawyers may remotely practice the law of the jurisdictions in which they are licensed while physically present in a jurisdiction in which they are not admitted if the local jurisdiction has not determined that the conduct is the unlicensed or unauthorized practice of law and if they do not hold themselves out as being licensed to practice in the local jurisdiction, do not advertise or otherwise hold out as having an office in the local jurisdiction, and do not provide or offer to provide legal services in the local jurisdiction. This practice may include the law of their licensing jurisdiction or other law as permitted by ABA Model Rule 5.5(c) or (d), including, for instance, temporary practice involving other states' or federal laws. Having local contact information on websites, letterhead, business cards, advertising, or the like would improperly establish a local office or local presence under the ABA Model Rules.[1]

Introduction

Lawyers, like others, have more frequently been working remotely: practicing law mainly through electronic means. Technology has made it possible for a lawyer to practice virtually in a jurisdiction where the lawyer is licensed, providing legal services to residents of that jurisdiction, even though the lawyer may be physically located in a different jurisdiction where the lawyer is not licensed. A lawyer's residence may not be the same jurisdiction where a lawyer is licensed. Thus, some lawyers have either chosen or been forced to remotely carry on their practice of the law of the jurisdiction or jurisdictions in which they are licensed while being physically present in a jurisdiction in which they are not licensed to practice. Lawyers may ethically engage in practicing law as authorized by their licensing jurisdiction(s) while being physically present in a jurisdiction in which they are not admitted under specific circumstances enumerated in this opinion.

Analysis

ABA Model Rule 5.5(a) prohibits lawyers from engaging in the unauthorized practice of law: "[a] lawyer shall not practice law in a jurisdiction in violation of the regulation of the legal profession in that jurisdiction, or assist another in doing so" unless authorized by the rules or law to do so. It is not this Committee's purview to determine matters of law; thus, this Committee will not opine whether working remotely by practicing the law of one's licensing jurisdiction in a particular jurisdiction where one is not licensed constitutes the unauthorized practice of law under the law of that jurisdiction. If a particular jurisdiction has made the determination, by statute, rule, case law, or opinion, that a lawyer working remotely while physically located in that jurisdiction constitutes

[1] This opinion is based on the ABA Model Rules of Professional Conduct as amended by the ABA House of Delegates through August 2020. The laws, court rules, regulations, rules of professional conduct, and opinions promulgated in individual jurisdictions are controlling.

the unauthorized or unlicensed practice of law, then Model Rule 5.5(a) also would prohibit the lawyer from doing so.

Absent such a determination, this Committee's opinion is that a lawyer may practice law pursuant to the jurisdiction(s) in which the lawyer is licensed (the "licensing jurisdiction") even from a physical location where the lawyer is not licensed (the "local jurisdiction") under specific parameters. Authorization in the licensing jurisdiction can be by licensure of the highest court of a state or a federal court. For purposes of this opinion, practice of the licensing jurisdiction law may include the law of the licensing jurisdiction and other law as permitted by ABA Model Rule 5.5(c) or (d), including, for instance, temporary practice involving other states' or federal laws. In other words, the lawyer may practice from home (or other remote location) whatever law(s) the lawyer is authorized to practice by the lawyer's licensing jurisdiction, as they would from their office in the licensing jurisdiction. As recognized by Rule 5.5(d)(2), a federal agency may also authorize lawyers to appear before it in any U.S. jurisdiction. The rules are considered rules of reason and their purpose must be examined to determine their meaning. Comment [2] indicates the purpose of the rule: "limiting the practice of law to members of the bar protects the public against rendition of legal services by unqualified persons." A local jurisdiction has no real interest in prohibiting a lawyer from practicing the law of a jurisdiction in which that lawyer is licensed and therefore qualified to represent clients in that jurisdiction. A local jurisdiction, however, does have an interest in ensuring lawyers practicing in its jurisdiction are competent to do so.

Model Rule 5.5(b)(1) prohibits a lawyer from "establish[ing] an office or other systematic and continuous presence in [the] jurisdiction [in which the lawyer is not licensed] for the practice of law." Words in the rules, unless otherwise defined, are given their ordinary meaning. "Establish" means "to found, institute, build, or bring into being on a firm or stable basis."[2] A local office is not "established" within the meaning of the rule by the lawyer working in the local jurisdiction if the lawyer does not hold out to the public an address in the local jurisdiction as an office and a local jurisdiction address does not appear on letterhead, business cards, websites, or other indicia of a lawyer's presence.[3] Likewise it does not "establish" a systematic and continuous presence in the jurisdiction for the practice of law since the lawyer is neither practicing the law of the local jurisdiction nor holding out the availability to do so. The lawyer's physical presence in the local jurisdiction is incidental; it is not for the practice of law. Conversely, a lawyer who includes a local jurisdiction address on websites, letterhead, business cards, or advertising may be said to have established an office or a systematic and continuous presence in the local jurisdiction for the practice of law.

Subparagraph (b)(2) prohibits a lawyer from "hold[ing] out to the public or otherwise represent[ing] that the lawyer is admitted to practice law in [the] jurisdiction" in which the lawyer is not admitted to practice. A lawyer practicing remotely from a local jurisdiction may not state or imply that the lawyer is licensed to practice law in the local jurisdiction. Again, information provided on websites, letterhead, business cards, or advertising would be indicia of whether a lawyer is "holding out" as practicing law in the local jurisdiction. If the lawyer's website,

[2] DICTIONARY.COM, https://www.dictionary.com/browse/establish?s=t (last visited Dec. 14, 2020).

[3] To avoid confusion of clients and others who might presume the lawyer is regularly present at a physical address in the licensing jurisdiction, the lawyer might include a notation in each publication of the address such as "by appointment only" or "for mail delivery."

letterhead, business cards, advertising, and the like clearly indicate the lawyer's jurisdictional limitations, do not provide an address in the local jurisdiction, and do not offer to provide legal services in the local jurisdiction, the lawyer has not "held out" as prohibited by the rule.

A handful of state opinions that have addressed the issue agree. Maine Ethics Opinion 189 (2005) finds:

> Where the lawyer's practice is located in another state and where the lawyer is working on office matters from afar, we would conclude that the lawyer is not engaged in the unauthorized practice of law. We would reach the same conclusion with respect to a lawyer who lived in Maine and worked out of his or her home for the benefit of a law firm and clients located in some other jurisdiction. In neither case has the lawyer established a professional office in Maine, established some other systematic and continuous presence in Maine, held himself or herself out to the public as admitted in Maine, or even provided legal services in Maine where the lawyer is working for the benefit of a non-Maine client on a matter focused in a jurisdiction other than Maine.

Similarly, Utah Ethics Opinion 19-03 (2019) states: "what interest does the Utah State Bar have in regulating an out-of-state lawyer's practice for out-of-state clients simply because he has a private home in Utah? And the answer is the same—none."

In addition to the above, Model Rule 5.5(c)(4) provides that lawyers admitted to practice in another United States jurisdiction and not disbarred or suspended from practice in any jurisdiction may provide legal services on a temporary basis in the local jurisdiction that arise out of or reasonably relate to the lawyer's practice in a jurisdiction where the lawyer is admitted to practice. Comment [6] notes that there is no single definition for what is temporary and that it may include services that are provided on a recurring basis or for an extended period of time. For example, in a pandemic that results in safety measures—regardless of whether the safety measures are governmentally mandated—that include physical closure or limited use of law offices, lawyers may temporarily be working remotely. How long that temporary period lasts could vary significantly based on the need to address the pandemic. And Model Rule 5.5(d)(2) permits a lawyer admitted in another jurisdiction to provide legal services in the local jurisdiction that they are authorized to provide by federal or other law or rule to provide. A lawyer may be subject to discipline in the local jurisdiction, as well as the licensing jurisdiction, by providing services in the local jurisdiction under Model Rule 8.5(a).

Conclusion

The purpose of Model Rule 5.5 is to protect the public from unlicensed and unqualified practitioners of law. That purpose is not served by prohibiting a lawyer from practicing the law of a jurisdiction in which the lawyer is licensed, for clients with matters in that jurisdiction, if the lawyer is for all intents and purposes invisible *as a lawyer* to a local jurisdiction where the lawyer is physically located, but not licensed. The Committee's opinion is that, in the absence of a local jurisdiction's finding that the activity constitutes the unauthorized practice of law, a lawyer may practice the law authorized by the lawyer's licensing jurisdiction for clients of that jurisdiction,

while physically located in a jurisdiction where the lawyer is not licensed if the lawyer does not hold out the lawyer's presence or availability to perform legal services in the local jurisdiction or actually provide legal services for matters subject to the local jurisdiction, unless otherwise authorized.

AMERICAN BAR ASSOCIATION

STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 498 **March 10, 2021**

Virtual Practice

The ABA Model Rules of Professional Conduct permit virtual practice, which is technologically enabled law practice beyond the traditional brick-and-mortar law firm.[1] *When practicing virtually, lawyers must particularly consider ethical duties regarding competence, diligence, and communication, especially when using technology. In compliance with the duty of confidentiality, lawyers must make reasonable efforts to prevent inadvertent or unauthorized disclosures of information relating to the representation and take reasonable precautions when transmitting such information. Additionally, the duty of supervision requires that lawyers make reasonable efforts to ensure compliance by subordinate lawyers and nonlawyer assistants with the Rules of Professional Conduct, specifically regarding virtual practice policies.*

I. Introduction

As lawyers increasingly use technology to practice virtually, they must remain cognizant of their ethical responsibilities. While the ABA Model Rules of Professional Conduct permit virtual practice, the Rules provide some minimum requirements and some of the Comments suggest best practices for virtual practice, particularly in the areas of competence, confidentiality, and supervision. These requirements and best practices are discussed in this opinion, although this opinion does not address every ethical issue arising in the virtual practice context.[2]

II. Virtual Practice: Commonly Implicated Model Rules

This opinion defines and addresses virtual practice broadly, as technologically enabled law practice beyond the traditional brick-and-mortar law firm.[3] A lawyer's virtual practice often occurs when a lawyer at home or on-the-go is working from a location outside the office, but a lawyer's practice may be entirely virtual because there is no requirement in the Model Rules that a lawyer

[1] This opinion is based on the ABA Model Rules of Professional Conduct as amended by the ABA House of Delegates through August 2020. The laws, court rules, regulations, rules of professional conduct, and opinions promulgated in individual jurisdictions are controlling.

[2] Interstate virtual practice, for instance, also implicates Model Rule of Professional Conduct 5.5: Unauthorized Practice of Law; Multijurisdictional Practice of Law, which is not addressed by this opinion. *See* ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 495 (2020), stating that "[l]awyers may remotely practice the law of the jurisdictions in which they are licensed while physically present in a jurisdiction in which they are not admitted if the local jurisdiction has not determined that the conduct is the unlicensed or unauthorized practice of law and if they do not hold themselves out as being licensed to practice in the local jurisdiction, do not advertise or otherwise hold out as having an office in the local jurisdiction, and do not provide or offer to provide legal services in the local jurisdiction."

[3] *See generally* MODEL RULES OF PROFESSIONAL CONDUCT R. 1.0(c), defining a "firm" or "law firm" to be "a lawyer or lawyers in a partnership, professional corporation, sole proprietorship or other association authorized to practice law; or lawyers employed in a legal services organization on the legal department of a corporation or other organization." Further guidance on what constitutes a firm is provided in Comments [2], [3], and [4] to Rule 1.0.

have a brick-and-mortar office. Virtual practice began years ago but has accelerated recently, both because of enhanced technology (and enhanced technology usage by both clients and lawyers) and increased need. Although the ethics rules apply to both traditional and virtual law practice,[4] virtual practice commonly implicates the key ethics rules discussed below.

A. Commonly Implicated Model Rules of Professional Conduct

1. Competence, Diligence, and Communication

Model Rules 1.1, 1.3, and 1.4 address lawyers' core ethical duties of competence, diligence, and communication with their clients. Comment [8] to Model Rule 1.1 explains, "To maintain the requisite knowledge and skill [to be competent], a lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology*, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject." (*Emphasis added*). Comment [1] to Rule 1.3 makes clear that lawyers must also "pursue a matter on behalf of a client despite opposition, obstruction or personal inconvenience to the lawyer, and take whatever lawful and ethical measures are required to vindicate a client's cause or endeavor." Whether interacting face-to-face or through technology, lawyers must "reasonably consult with the client about the means by which the client's objectives are to be accomplished; . . . keep the client reasonably informed about the status of the matter; [and] promptly comply with reasonable requests for information. . . ."[5] Thus, lawyers should have plans in place to ensure responsibilities regarding competence, diligence, and communication are being fulfilled when practicing virtually.[6]

2. Confidentiality

Under Rule 1.6 lawyers also have a duty of confidentiality to all clients and therefore "shall not reveal information relating to the representation of a client" (absent a specific exception, informed consent, or implied authorization). A necessary corollary of this duty is that lawyers must at least "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."[7] The following non-

[4] For example, if a jurisdiction prohibits substantive communications with certain witnesses during court-related proceedings, a lawyer may not engage in such communications either face-to-face or virtually (e.g., during a trial or deposition conducted via videoconferencing). *See, e.g.*, MODEL RULES OF PROF'L CONDUCT R. 3.4(c) (prohibiting lawyers from violating court rules and making no exception to the rule for virtual proceedings). Likewise, lying or stealing is no more appropriate online than it is face-to-face. *See, e.g.*, MODEL RULES OF PROF'L CONDUCT R. 1.15; MODEL RULES OF PROF'L CONDUCT R. 8.4(b)-(c).

[5] MODEL RULES OF PROF'L CONDUCT R. 1.4(a)(2) – (4).

[6] Lawyers unexpectedly thrust into practicing virtually must have a business continuation plan to keep clients apprised of their matters and to keep moving those matters forward competently and diligently. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 482 (2018) (discussing ethical obligations related to disasters). Though virtual practice is common, if for any reason a lawyer cannot fulfill the lawyer's duties of competence, diligence, and other ethical duties to a client, the lawyer must withdraw from the matter. MODEL RULES OF PROF'L CONDUCT R. 1.16. During and following the termination or withdrawal process, the "lawyer shall take steps to the extent reasonably practicable to protect a client's interests, such as giving reasonable notice to the client, allowing time for employment of other counsel, surrendering papers and property to which the client is entitled and refunding any advance payment of fee or expense that has not been earned or incurred." MODEL RULES OF PROF'L CONDUCT R. 1.16(d).

[7] MODEL RULES OF PROF'L CONDUCT R. 1.6(c).

exhaustive list of factors may guide the lawyer's determination of reasonable efforts to safeguard confidential information: "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)."[8] As ABA Formal Op. 477R notes, lawyers must employ a "fact-based analysis" to these "nonexclusive factors to guide lawyers in making a 'reasonable efforts' determination."

Similarly, lawyers must take reasonable precautions when transmitting communications that contain information related to a client's representation.[9] At all times, but especially when practicing virtually, lawyers must fully consider and implement reasonable measures to safeguard confidential information and take reasonable precautions when transmitting such information. This responsibility "does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy."[10] However, depending on the circumstances, lawyers may need to take special precautions.[11] Factors to consider to assist the lawyer in determining the reasonableness of the "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."[12] As ABA Formal Op. 477R summarizes, "[a] lawyer generally may transmit information relating to the representation of a client over the Internet without violating the Model Rules of Professional Conduct where the lawyer has undertaken reasonable efforts to prevent inadvertent or unauthorized access."

3. Supervision

Lawyers with managerial authority have ethical obligations to establish policies and procedures to ensure compliance with the ethics rules, and supervisory lawyers have a duty to make reasonable efforts to ensure that subordinate lawyers and nonlawyer assistants comply with the applicable Rules of Professional Conduct.[13] Practicing virtually does not change or diminish this obligation. "A lawyer must give such assistants appropriate instruction and supervision concerning the ethical aspects of their employment, particularly regarding the obligation not to disclose information relating to representation of the client, and should be responsible for their work product."[14] Moreover, a lawyer must "act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent

[8] MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. [18].
[9] MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. [19].
[10] *Id.*
[11] The opinion cautions, however, that "a lawyer may be required to take special security precautions to protect against the inadvertent or unauthorized disclosure of client information when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security." ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R (2017).
[12] MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. [19].
[13] MODEL RULES OF PROF'L CONDUCT R. 5.1 & 5.3. *See, e.g.,* ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 467 (2014) (discussing managerial and supervisory obligations in the context of prosecutorial offices). *See also* ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 483 n.6 (2018) (describing the organizational structures of firms as pertaining to supervision).
[14] MODEL RULES OF PROF'L CONDUCT R. 5.3 cmt. [2].

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*."[15] The duty to supervise nonlawyers extends to those both within and outside of the law firm.[16]

B. Particular Virtual Practice Technologies and Considerations

Guided by the rules highlighted above, lawyers practicing virtually need to assess whether their technology, other assistance, and work environment are consistent with their ethical obligations. In light of current technological options, certain available protections and considerations apply to a wide array of devices and services. As ABA Formal Op. 477R noted, a "lawyer has a variety of options to safeguard communications including, for example, using secure internet access methods to communicate, access and store client information (such as through secure Wi-Fi, the use of a Virtual Private Network, or another secure internet portal), using unique complex passwords, changed periodically, implementing firewalls and anti-Malware/Anti-Spyware/Antivirus software on all devices upon which client confidential information is transmitted or stored, and applying all necessary security patches and updates to operational and communications software." Furthermore, "[o]ther available tools include encryption of data that is physically stored on a device and multi-factor authentication to access firm systems." To apply and expand on these protections and considerations, we address some common virtual practice issues below.

1. Hard/Software Systems

Lawyers should ensure that they have carefully reviewed the terms of service applicable to their hardware devices and software systems to assess whether confidentiality is protected.[17] To protect confidential information from unauthorized access, lawyers should be diligent in installing any security-related updates and using strong passwords, antivirus software, and encryption. When connecting over Wi-Fi, lawyers should ensure that the routers are secure and should consider using virtual private networks (VPNs). Finally, as technology inevitably evolves, lawyers should periodically assess whether their existing systems are adequate to protect confidential information.

---

[15] MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. [18] (emphasis added).

[16] As noted in Comment [3] to Model Rule 5.3:

> When using such services outside the firm, a lawyer must make reasonable efforts to ensure that the services are provided in a manner that is compatible with the lawyer's professional obligations. The extent of this obligation will depend upon the circumstances, including the education, experience and reputation of the nonlawyer; the nature of the services involved; the terms of any arrangements concerning the protection of client information; and the legal and ethical environments of the jurisdictions in which the services will be performed, particularly with regard to confidentiality. See also Rules 1.1 (competence), 1.2 (allocation of authority), 1.4 (communication with client), 1.6 (confidentiality), 5.4(a) (professional independence of the lawyer), and 5.5(a) (unauthorized practice of law).

[17] For example, terms and conditions of service may include provisions for data-soaking software systems that collect, track, and use information. Such systems might purport to own the information, reserve the right to sell or transfer the information to third parties, or otherwise use the information contrary to lawyers' duty of confidentiality.

2. Accessing Client Files and Data

Lawyers practicing virtually (even on short notice) must have reliable access to client contact information and client records. If the access to such "files is provided through a cloud service, the lawyer should (i) choose a reputable company, and (ii) take reasonable steps to ensure that the confidentiality of client information is preserved, and that the information is readily accessible to the lawyer."[18] Lawyers must ensure that data is regularly backed up and that secure access to the backup data is readily available in the event of a data loss. In anticipation of data being lost or hacked, lawyers should have a data breach policy and a plan to communicate losses or breaches to the impacted clients.[19]

3. Virtual meeting platforms and videoconferencing

Lawyers should review the terms of service (and any updates to those terms) to ensure that using the virtual meeting or videoconferencing platform is consistent with the lawyer's ethical obligations. Access to accounts and meetings should be only through strong passwords, and the lawyer should explore whether the platform offers higher tiers of security for businesses/enterprises (over the free or consumer platform variants). Likewise, any recordings or transcripts should be secured. If the platform will be recording conversations with the client, it is inadvisable to do so without client consent, but lawyers should consult the professional conduct rules, ethics opinions, and laws of the applicable jurisdiction.[20] Lastly, any client-related meetings or information should not be overheard or seen by others in the household, office, or other remote location, or by other third parties who are not assisting with the representation,[21] to avoid jeopardizing the attorney-client privilege and violating the ethical duty of confidentiality.

4. Virtual Document and Data Exchange Platforms

In addition to the protocols noted above (e.g., reviewing the terms of service and any updates to those terms), lawyers' virtual document and data exchange platforms should ensure that

---

[18] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 482 (2018).

[19] *See, e.g.*, ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 483 (2018) ("Even lawyers who, (i) under Model Rule 1.6(c), make 'reasonable efforts to prevent the . . . unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client,' (ii) under Model Rule 1.1, stay abreast of changes in technology, and (iii) under Model Rules 5.1 and 5.3, properly supervise other lawyers and third-party electronic-information storage vendors, may suffer a data breach. When they do, they have a duty to notify clients of the data breach under Model Rule 1.4 in sufficient detail to keep clients 'reasonably informed' and with an explanation 'to the extent necessary to permit the client to make informed decisions regarding the representation.'").

[20] *See, e.g.*, ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 01-422 (2001).

[21] Pennsylvania recently highlighted the following best practices for videoconferencing security:

- Do not make meetings public;
- Require a meeting password or use other features that control the admittance of guests;
- Do not share a link to a teleconference on an unrestricted publicly available social media post;
- Provide the meeting link directly to specific people;
- Manage screensharing options. For example, many of these services allow the host to change screensharing to "Host Only;"
- Ensure users are using the updated version of remote access/meeting applications.

Pennsylvania Bar Ass'n Comm. on Legal Ethics & Prof'l Responsibility, Formal Op. 2020-300 (2020) (citing an FBI press release warning of teleconference and online classroom hacking).

documents and data are being appropriately archived for later retrieval and that the service or platform is and remains secure. For example, if the lawyer is transmitting information over email, the lawyer should consider whether the information is and needs to be encrypted (both in transit and in storage).[22]

5. Smart Speakers, Virtual Assistants, and Other Listening-Enabled Devices

Unless the technology is assisting the lawyer's law practice, the lawyer should disable the listening capability of devices or services such as smart speakers, virtual assistants, and other listening-enabled devices while communicating about client matters. Otherwise, the lawyer is exposing the client's and other sensitive information to unnecessary and unauthorized third parties and increasing the risk of hacking.

6. Supervision

The virtually practicing managerial lawyer must adopt and tailor policies and practices to ensure that all members of the firm and any internal or external assistants operate in accordance with the lawyer's ethical obligations of supervision.[23] Comment [2] to Model Rule 5.1 notes that "[s]uch policies and procedures include those designed to detect and resolve conflicts of interest, identify dates by which actions must be taken in pending matters, account for client funds and property and ensure that inexperienced lawyers are properly supervised."

a. Subordinates/Assistants

The lawyer must ensure that law firm tasks are being completed in a timely, competent, and secure manner.[24] This duty requires regular interaction and communication with, for example,

---

[22] *See, e.g.*, ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R (2017) (noting that "it is not always reasonable to rely on the use of unencrypted email").

[23] As ABA Formal Op. 477R noted:

> In the context of electronic communications, lawyers must establish policies and procedures, and periodically train employees, subordinates and others assisting in the delivery of legal services, in the use of reasonably secure methods of electronic communications with clients. Lawyers also must instruct and supervise on reasonable measures for access to and storage of those communications. Once processes are established, supervising lawyers must follow up to ensure these policies are being implemented and partners and lawyers with comparable managerial authority must periodically reassess and update these policies. This is no different than the other obligations for supervision of office practices and procedures to protect client information.

[24] The New York County Lawyers Association Ethics Committee recently described some aspects to include in the firm's practices and policies:

- Monitoring appropriate use of firm networks for work purposes.
- Tightening off-site work procedures to ensure that the increase in worksites does not similarly increase the entry points for a data breach.
- Monitoring adherence to firm cybersecurity procedures (e.g., not processing or transmitting work across insecure networks, and appropriate storage of client data and work product).
- Ensuring that working at home has not significantly increased the likelihood of an inadvertent disclosure through misdirection of a transmission, possibly because the lawyer or nonlawyer was distracted by a child, spouse, parent or someone working on repair or maintenance of the home.

associates, legal assistants, and paralegals. Routine communication and other interaction are also advisable to discern the health and wellness of the lawyer's team members.[25]

One particularly important subject to supervise is the firm's bring-your-own-device (BYOD) policy. If lawyers or nonlawyer assistants will be using their own devices to access, transmit, or store client-related information, the policy must ensure that security is tight (e.g., strong passwords to the device and to any routers, access through VPN, updates installed, training on phishing attempts), that any lost or stolen device may be remotely wiped, that client-related information cannot be accessed by, for example, staff members' family or others, and that client-related information will be adequately and safely archived and available for later retrieval.[26]

Similarly, all client-related information, such as files or documents, must not be visible to others by, for example, implementing a "clean desk" (and "clean screen") policy to secure documents and data when not in use. As noted above in the discussion of videoconferencing, client-related information also should not be visible or audible to others when the lawyer or nonlawyer is on a videoconference or call. In sum, all law firm employees and lawyers who have access to client information must receive appropriate oversight and training on the ethical obligations to maintain the confidentiality of such information, including when working virtually.

b. Vendors and Other Assistance

Lawyers will understandably want and may need to rely on information technology professionals, outside support staff (e.g., administrative assistants, paralegals, investigators), and vendors. The lawyer must ensure that all of these individuals or services comply with the lawyer's obligation of confidentiality and other ethical duties. When appropriate, lawyers should consider use of a confidentiality agreement,[27] and should ensure that all client-related information is secure, indexed, and readily retrievable.

7. Possible Limitations of Virtual Practice

Virtual practice and technology have limits. For example, lawyers practicing virtually must make sure that trust accounting rules, which vary significantly across states, are followed.[28] The

---

- Ensuring that sufficiently frequent "live" remote sessions occur between supervising attorneys and supervised attorneys to achieve effective supervision as described in [New York Rule of Professional Conduct] 5.1(c).

N.Y. County Lawyers Ass'n Comm. on Prof'l Ethics, Formal Op. 754-2020 (2020).

[25] *See* ABA MODEL REGULATORY OBJECTIVES FOR THE PROVISION OF LEGAL SERVICES para. I (2016).

[26] For example, a lawyer has an obligation to return the client's file when the client requests or when the representation ends. *See, e.g.*, MODEL RULES OF PROF'L CONDUCT R. 1.16(d). This important obligation cannot be fully discharged if important documents and data are located in staff members' personal computers or houses and are not indexed or readily retrievable by the lawyer.

[27] *See, e.g.*, Mo. Bar Informal Advisory Op. 20070008 & 20050068.

[28] *See* MODEL RULES OF PROF'L CONDUCT R. 1.15; *See, e.g.*, ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 482 (2018) ("Lawyers also must take reasonable steps in the event of a disaster to ensure access to funds the lawyer is holding in trust. A lawyer's obligations with respect to these funds will vary depending on the circumstances. Even before a disaster, all lawyers should consider (i) providing for another trusted signatory on trust

lawyer must still be able, to the extent the circumstances require, to write and deposit checks, make electronic transfers, and maintain full trust-accounting records while practicing virtually. Likewise, even in otherwise virtual practices, lawyers still need to make and maintain a plan to process the paper mail, to docket correspondence and communications, and to direct or redirect clients, prospective clients, or other important individuals who might attempt to contact the lawyer at the lawyer's current or previous brick-and-mortar office. If a lawyer will not be available at a physical office address, there should be signage (and/or online instructions) that the lawyer is available by appointment only and/or that the posted address is for mail deliveries only. Finally, although e-filing systems have lessened this concern, litigators must still be able to file and receive pleadings and other court documents.

III. Conclusion

The ABA Model Rules of Professional Conduct permit lawyers to conduct practice virtually, but those doing so must fully consider and comply with their applicable ethical responsibilities, including technological competence, diligence, communication, confidentiality, and supervision.

accounts in the event of the lawyer's unexpected death, incapacity, or prolonged unavailability and (ii) depending on the circumstances and jurisdiction, designating a successor lawyer to wind up the lawyer's practice.").

Speaker Bios

Buchalter

Caroline Djang

Orange County, California
Shareholder

P (949) 224-6252
F (949) 720-0182
cdjang@buchalter.com

Areas of Practice & Industry Specialties
Insolvency & Financial Law Group; Litigation; Sports Industry Law

---

Caroline Djang is member of Buchalter's Insolvency and Financial Law practice group in the Firm's Orange County office. Ms. Djang practices in the areas of insolvency, bankruptcy, and litigation. She has vast experience representing various creditors, trustees, debtors, and committees in bankruptcy cases and adversary proceedings. Ms. Djang is a Chapter 11 Subchapter V Trustee for the Central District of California. She counsels her clients on the best strategies for pursuing and collecting debts and realistically advises them on their prospects for recovery. She also helps her clients in financial distress to understand their options. Ms. Djang is a frequent speaker on the Small Business Reorganization Act.

Ms. Djang is a certified mediator and is serving by appointment to the Bankruptcy Mediation Program Panel for the U.S. Central District of California Bankruptcy Court. She is also an At-Large Member of the Ninth Circuit Conference Executive Committee, Board Member of the Orange County Bar Association, Commercial Law and Bankruptcy Section and Treasurer of the Orange County Women Lawyers Association. Prior to entering into private practice, Ms. Djang was a judicial law clerk at the U.S. Bankruptcy Court for seven years, clerking for U.S. Bankruptcy Judges Ellen Carroll, Vincent P. Zurzolo, Sheri Bluebond and Richard M. Neiter.

Ms. Djang's honors and recognitions include:

- Banking and Finance Visionary, *Los Angeles Times*, 2021
- *Southern California Super Lawyers,* Bankruptcy, 2017-2023
- *Southern California Super Lawyers* Orange County Top 50, 2021-23
- *Southern California Super Lawyers* Top 50 Women Attorneys, 2022 -2023
- *Southern California Super Lawyers* Top 100, 2022-2023
- The Best Lawyers in America®, Litigation – Bankruptcy and Bankruptcy and Creditor Debtor Rights/Insolvency and Reorganization, 2020-2022
- Litigation – Bankruptcy Lawyer of the Year in Irvine, Best Lawyers®, 2020
- Up-and-Coming 25: 2015 Orange County Rising Stars
- Up-and-Coming 50: 2015 Women Southern California Rising Stars
- Up-and-Coming 100: 2015 Southern California Rising Stars
- *Southern California Super Lawyers Rising Stars*, Bankruptcy, 2011-2012, 2014-2015
- Top Attorneys, 2014, 2015 (10.0 Avvo ranking) OC Metro Magazine Orange County Register's
- Lawyers of Color's Inaugural Hot List (Western Region), 2013

Prior Affiliations

- Jeffer Mangels Butler & Mitchell LLP

- Rutan & Tucker LLP
- Best Best & Krieger LLP

Representative Matters

- Represent several Chapter 7 trustees as both general and special litigation counsel in various bankruptcy cases and adversary proceedings.
- Represent several prominent landlords in California with respect to landlords' and creditors' rights and claims in bankruptcy.
- Represent an internationally-known luxury brand with respect to creditors' rights.
- Represent numerous cities and municipalities with respect to creditors' rights and claims in bankruptcy.
- Serve as local California bankruptcy counsel to a major national bank.
- Represented one of the largest creditors in the chapter 11 case of a recycling company.
- Represented an issuer of bonds in connection with the chapter 11 case of a HERO loan servicer.
- Represented a secured creditor in a plan confirmation trial that resulted in a consensual confirmed Chapter 11 plan.
- Represented the Official Committee of Unsecured Creditors of a music-sharing website. Prosecuted avoidance actions, resulting in substantial recovery to the Chapter 11 estate.
- Represented the debtor, a construction company located in Central California, in its Chapter 11 case. Unsecured creditors were paid in full, and the secured lender obtained a substantial recovery.
- Prevailed on appeal on behalf of a counterparty to an executory contract, which was rejected by a state court receiver.
- Represented a prepetition secured lender in a Chapter 11 case in the District of Delaware, which resulted in payment in full to the lender through a section 363 sale of assets.
- Represented more than 40 similarly situated defendants in fraudulent transfer litigation, which resulted in dismissal with prejudice of the actions and allowed claims for each defendant. Defeated Chapter 11 plan confirmation of a single asset real estate debtor and obtained relief from the automatic stay on behalf of a secured lender.
- Represented a major title company in settling a potential multi-million dollar claim by a Chapter 7 trustee.
- Represented the Chapter 11 trustee in a high-profile Ponzi scheme case in the U.S. Bankruptcy Court for the Central District of California.
- Represented a San Diego-based bottled water company in its Chapter 11 case. Confirmed a Chapter 11 plan and settled contentious litigation.
- Represented the Chapter 11 trustee in a large real estate case in Santa Barbara.
- Confirmed a Chapter 11 liquidating plan for a ramen company in Orange County.
- Settled and obtained dismissals in numerous avoidance actions on behalf of defendants.
- Represented numerous creditors, including landlords and holders of reclamation and section 503(b)(9) claims, in several major bankruptcy cases, such as Sears, Hertz, 24 Hour Fitness, PG&E, Circuit City, Lehman Brothers and Radio Shack.
- Represented one of the largest food service companies in Orange County.

Publications

- Five Takeaways for Commercial Landlords When Tenants File Bankruptcy, *BB&K Legal Alerts*, July 8, 2020
- Debunking the Sham Guaranty Defense, *State Bar of California Real Property Section, E-Bulletin*, November 2016

- In Rem Relief from Stay - Affords Relief from Serial Bankruptcies for Real Estate Lenders, *Orange County Business Journal*, November 2015
- Real Estate Lenders Relief From Serial Bankruptcies - aka “In Rem” Relief From Stay, *California Mortgage Finance News*, Spring 2014
- Singled Out - Chapter 11 Provides Only Temporary Respite to an Entity in a Single Asset Real Estate Bankruptcy, *Los Angeles Lawyer*, January 2012
- Stern v. Marshall Bankruptcy Case: Bombshell or Dud? (Part I and II), *Los Angeles Daily Journal*, October 2011
- Volunteer Attorney Program Can Alleviate Bankruptcy Court’s Massive Workload, *Los Angeles Daily Journal*, February 2011

Presentations

- Speaker, "Subchapter V’s Greatest Hits," California Bankruptcy Forum Insolvency Conference, June 1, 2022
- Speaker, "Covid Update on Restructuring and Recovery Options," Turnaround Management Association – Southern California and the California Receivers Forum, April 1, 2022
- Speaker, "The New Small Business Reorganization Act (SBRA) – Why Consumer Bankruptcy Attorneys Need to Understand Sub-Chapter V," National Association of Consumer Bankruptcy Attorneys; , December 1, 2021
- Speaker, "A Chapter 11 Primer," National Association of Consumer Bankruptcy Attorneys, November 1, 2021
- Speaker, "DEI and Judicial Clerkships," Southwestern Law School, October 1, 2021
- Speaker, "First Look at Small Business Reorganization Act Cases," American Bankruptcy Institute Southwest Conference, August 1, 2021
- Speaker, "The Small Business Reorganization Act of 2019," Association of Insolvency and Restructuring Professionals, June 1, 2021
- Speaker, "Walk the Plank: Debates on Hot Topics in Bankruptcy," California Bankruptcy Forum Insolvency Conference 2021, May 1, 2021
- Speaker, "One Year Later: Retrospection on Sub-Chapter V Bankruptcy Practice," California Lawyers Association – Insolvency Law Committee, April 1, 2021
- Speaker, "A Leaky Boat On A Choppy Sea: A Very Timely Bankruptcy Primer For Small Businesses," Los Angeles County Bar Association, March 1, 2021
- Speaker, "One Year Into SBRA: Meet The Subchapter V Trustees," Central District Consumer Bankruptcy Attorney Association, February 1, 2021
- Speaker, "Subchapter V…So Far," Orange County Bankruptcy Forum, September 1, 2020
- Speaker, "How to Reorganize a Small Business Under the Recent Amendments to Chapter 11," Inland Empire Bankruptcy Forum, March 1, 2020
- Speaker, "California Lawyers Association Business Law Section Diversity Roadshow," California State University Fullerton, December 1, 2019
- Speaker, "Advanced Civil Procedures," Riverside County Sheriff’s Department, February 1, 2018
- Moderator, "Judges’ Night," Orange County Bankruptcy Forum, October 1, 2017

Education

Ms. Djang earned her J.D. from Loyola Law School, and her B.A. in English from the University of Pennsylvania.

Bar Admissions

- California

Community

- Orange County Bar Association, Board Member
- Certified mediator, serving by appointment to the Bankruptcy Mediation Program Panel for the U.S. Central District of California Bankruptcy Court
- At-Large Member of the Ninth Circuit Conference Executive Committee
- Orange County Bar Association: Commercial Law and Bankruptcy Section Chair; Diversity and Inclusion Committee
- Orange County Women's Law Association, Treasurer
- Orange County Bankruptcy Forum, former Board of Directors and past president
- ABI Battleground West, 2020 Advisory Board
- California Bankruptcy Forum Insolvency Conference Co-Chair, 2016-2017
- Orange County Asian American Bar Association, Member
- Central District of California Small Business Reorganization Task Force Member, 2020-2021
- Inland Empire Bankruptcy Forum, Member
- Federal Exploration Day, Attorney Participant, 2018, 2019
- Coro Women in Leadership, Advisory Committee
- Community Legal Aid of SoCal: Justice Is Served Committee

Joseph R. Dunn, Mintz
Member – Bankruptcy & Restructuring
Co-Chair – Cross-Border Asset Recovery Practice

Joe is a Member at Mintz in the Bankruptcy & Restructuring Practice, and Co-Chair of the Cross-Border Asset Recovery Practice. As a seasoned bankruptcy and creditor rights litigator, Joe has developed a unique practice in asset recovery, judgment enforcement, and litigation in the insolvency arena. Joe's broad-ranging litigation and restructuring practice draws on his significant experience with complex creditor rights litigation, bankruptcy litigation, and other work in insolvency scenarios. He has a long track record of successfully representing institutional creditors, bankruptcy trustees, litigation trustees, and other fiduciaries in investigating and pursuing complex asset recovery matters, often through litigation focused on piercing fraudulent schemes and offshore asset protection devices. Institutional investors, hedge funds, and large financial institutions value his counsel. While based in San Diego for the past 15 years, Joe's practice spans the globe and he regularly practices in courts around the country.

United States Bankruptcy Judge Ronald H. Sargis attended Stanford University and graduated in 1979 with a bachelor's degree. In 1982, Judge Sargis completed his Juris Doctor Degree, with distinction, at the University of the Pacific, McGeorge School of Law. Following law school, Judge Sargis served as a Law Clerk to the Honorable Loren Dahl, United States Bankruptcy Judge, Eastern District of California. Judge Sargis subsequently served in private practice for 26 years, during which time he became a partner at Hefner, Stark & Marois. In addition to bankruptcy law, Judge Sargis' legal practice included commercial law, PACA litigation, fair debt collection practices and fair credit reporting compliance and litigation, oil and gas law, and federal and state legislation and regulation relating to fair debt collection practices, fair credit reporting, homestead, and other exemptions, and HIPPA regulations and compliance. He also served as Chancellor for St. Michael's Church and as the Church Attorney for the Episcopal Diocese of Northern California. His appellate practice was before the Bankruptcy Appellate Panel, U.S. District Court, Ninth Circuit Court of Appeals, California District Court of Appeal, and the California Supreme Court.

On January 14, 2010, Judge Sargis was appointed to serve as a United States Bankruptcy Judge for the Eastern District of California. Judge Sargis served a seven-year term as Chief Bankruptcy Judge for the Eastern District of California, served on the Ninth Circuit Conference of Chief Bankruptcy Judges Committee during that period, served for three years on the Executive Committee for that Conference, and served as the Chair of that Conference for the 2021-2022 year, during which he was the Chief Bankruptcy Judge Observer to the Ninth Circuit Judicial Council and the Ninth Circuit District Court Judges Conference. Judge Sargis has also served on the California State-Federal Judicial Council. Judge Sargis was an Adjunct Professor of the Bankruptcy Course at the McGeorge School of law from 2014 to 2020. Additionally, Judge Sargis serves on the Legislative Committee for the National Conference of Bankruptcy Judges.