



The State Bar of California

OPEN SESSION AGENDA ITEM SEPTEMBER 2020 REGULATION AND DISCIPLINE COMMITTEE II.B

DATE: September 24, 2020

TO: Members, Regulation and Discipline Committee

FROM: Andrew Tuft, Supervising Attorney, Office of Professional Competence

SUBJECT: Formal Advisory Ethics Opinion 2020-203: Request for Approval for Publication

EXECUTIVE SUMMARY

This agenda item seeks Board Committee on Regulation and Discipline (RAD) approval for the publication of proposed Formal Ethics Advisory Opinion 2020-203 developed by the Committee on Professional Responsibility and Conduct (COPRAC or the committee), following the close of two public comment periods.

BACKGROUND

COPRAC is charged with developing the State Bar's nonbinding, advisory ethics opinions.¹ Authority to approve the issuance of an ethics opinion is exercised by RAD in accordance with applicable State Bar policy and procedure,² which provides that once the committee has approved a formal opinion following consideration of public comment, the formal opinion and the issue of whether the formal opinion shall be published shall be placed on the agenda of the next succeeding meeting of RAD for decision.

¹ Each published opinion includes the following statement: "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 on 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." Although nonbinding, State Bar formal ethics opinions have been cited by the California courts in analyzing issues of attorney professional responsibility. (See, e.g., *Huskinson & Brown v. Wolf* (2004) 32 Cal.4th 453, 459.)

² See Board Resolutions, July 1979, December 2004, and November 2016.

DISCUSSION

This agenda item requests approval for the publication of Proposed Formal Advisory Ethics Opinion 2020-203. Prior to being finalized for publication, while the opinion was still in development and out for public comment, it was designated as Proposed Formal Opinion Interim No. 16-0002.

Proposed Formal Opinion Interim No. 16-0002 was drafted by COPRAC and at its December 6, 2019 meeting, in accordance with COPRAC's procedures, the committee approved the opinion for an initial 90-day public comment distribution.³ Subsequently, at its April 16, 2020 meeting, COPRAC revised the opinion in response to public comments received and approved a further 60-day public comment period.

The full text of the proposed opinion is provided as Attachment A. The question addressed in the proposed opinion is: "What are a lawyer's ethical obligations with respect to unauthorized access by third persons to electronically stored confidential client information in the lawyer's possession?" The opinion digest states:

Lawyers who use electronic devices which contain confidential client information must assess the risks of keeping such data on electronic devices and computers, and take reasonable steps to secure their electronic systems to minimize the risk of unauthorized access. In the event of a breach, lawyers have an obligation to conduct a reasonable inquiry to determine the extent and consequences of the breach and to notify any client whose interests have a reasonable possibility of being negatively impacted by the breach.

Public Comment

In response to the second public comment period that ended on June 24, 2020, four public comments were received and are provided as Attachment B.

The Los Angeles County Bar Association Professional Responsibility and Ethics Committee (LACBA) stated they agree with much of the proposed opinion and offered a few nonsubstantive edits to the opinion, the majority of which the committee accepted. LACBA also expressed concern regarding the phrase that a lawyer must "minimize the risk of unauthorized access" to data contained on electronic devices because LACBA believes "minimize" means "reduce (something, especially something unwanted or unpleasant) to the smallest degree possible." They believe "minimize" infers a standard of perfection; when a "reasonableness" standard is more appropriate. The committee believes the standard is properly stated in the opinion's digest as follows: "Lawyers who use electronic devices which contain confidential client information must assess the risks of keeping such data on electronic devices and computers, and take reasonable steps to secure their electronic systems to minimize the risk of unauthorized access." The committee believes the opinion conveys the lawyer's duty is one of

³ See Board Resolution, December 2004.

reasonableness under the circumstances to address risk, and that the opinion should not be read to suggest that the lawyer has an unqualified or absolute duty to completely prevent or eliminate the risk of unauthorized access to electronically stored confidential information. However, to offer further clarity in this area, the committee added the following revised sentence to the opinion: “‘Reasonable efforts’ are those which are reasonably calculated under the circumstances to minimize particular identified risks.”

The Orange County Bar Association (OCBA) stated they believe the opinion provides valuable guidance. However, OCBA disagreed with following statement contained in Footnote 6: “This opinion focuses on current clients and does not address the duty of disclosure owed to former clients. The committee agrees with the discussion of this issue in ABA Formal Opn. No. 18-483, and does not believe that California’s rule 1.9 imposes a duty to notify a former client of a data breach, although other applicable law may require notification.” OCBA requested that although rule 1.9 may not require disclosure to a former client, other ethical obligations or rules could require disclosure depending on the circumstances. OCBA requested that the committee amend this footnote and adopt a more nuanced approach. The committee agreed and amended the footnote by—among other things—adding a citation to Maine Professional Ethics Commission Opinion No. 220, which concludes that a lawyer must notify a former client concerning a data breach under certain circumstances.

Felicia Williams submitted a comment indicating support for the opinion as drafted.

Mina Sirkin submitted a comment in opposition to the opinion, stating it would put too large a burden on lawyers and that once a breach occurs and the data has been compromised, there is very little a lawyer can do. The committee believes the opinion states the appropriate standard for lawyers, which is: for those lawyers who choose to use electronic devices to store confidential client information, they must assess the risks associated with that practice and take reasonable steps under the circumstances to minimize particular identified risks. With respect to the lawyer’s duty after a breach occurs, the committee believes the opinion appropriately describes the lawyer’s obligation as having to conduct a reasonable inquiry in order to determine the extent of the breach, and to notify any client whose interests have a reasonable possibility of being negatively impacted by the breach.

At its July 24, 2020 meeting, following consideration of the public comment received, COPRAC approved the opinion for submission to RAD for formal publication. The State Bar Standing Committee on Professional Responsibility and Conduct requests that RAD approve the publication of Formal Ethics Advisory Opinion No. 2020-203.

FISCAL/PERSONNEL IMPACT

None

AMENDMENTS TO RULES OF THE STATE BAR

None

AMENDMENTS TO BOARD OF TRUSTEES POLICY MANUAL

None

STRATEGIC PLAN GOALS & OBJECTIVES

Goal: None

RECOMMENDATIONS

Should the Regulation and Discipline Committee concur in the proposed action, passage of the following resolution is recommended:

RESOLVED, that the Board of Trustees Regulation and Discipline Committee; following publication for public comment and consideration of the comments received, and upon the recommendation of the State Bar Standing Committee on Professional Responsibility and Conduct, approves the publication of Formal Ethics Advisory Opinion 2020-203, attached hereto as Attachment A.

ATTACHMENT(S) LIST

- A.** Formal Ethics Advisory Opinion 2020-203
- B.** Full Text of Public Comments

**THE STATE BAR OF CALIFORNIA
STANDING COMMITTEE ON
PROFESSIONAL RESPONSIBILITY AND CONDUCT
FORMAL OPINION NO. 2020-203**

ISSUE: What are a lawyer’s ethical obligations with respect to unauthorized access by third persons to electronically stored confidential client information in the lawyer’s possession?

DIGEST: Lawyers who use electronic devices which contain confidential client information must assess the risks of keeping such data on electronic devices and computers, and take reasonable steps to secure their electronic systems to minimize the risk of unauthorized access. In the event of a breach, lawyers have an obligation to conduct a reasonable inquiry to determine the extent and consequences of the breach and to notify any client whose interests have a reasonable possibility of being negatively impacted by the breach.

AUTHORITIES

INTERPRETED: Rules 1.1, 1.4, 1.6, 5.1, 5.2, and 5.3 of the Rules of Professional Conduct of the State Bar of California.^{1/}

Business and Professions Code sections 6068(e) and 6068(m).

Civil Code section 1798.82.

INTRODUCTION

Data breaches resulting from lost, stolen or hacked electronic devices and systems are a reality in today’s world. There are important ethical concerns when data breaches happen to lawyers and law firms since such events may involve the potential loss of, or unauthorized access to, confidential client information^{2/} and, thus, may require a lawyer to take certain remedial steps to protect the client.

In Cal. State Bar Formal Opn. No. 2015-193, the Committee on Professional Responsibility and Conduct (“Committee”) discussed lawyers’ ethical obligations when dealing with e-discovery. In

^{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/} The phrase “confidential client information” in this opinion includes not only attorney-client privileged communications, but more broadly all client information protected from disclosure under Business and Profession Code section 6068(e)(1) and rule 1.6.

Cal. State Bar Formal Opn. No. 2010-179, the Committee discussed ethical issues that arise when a lawyer accesses confidential client information on a laptop over public Wi-Fi or a home Wi-Fi network. In both opinions, the Committee adopted an approach that posed questions lawyers should consider in order to comply with the duties of competence and confidentiality. In light of ever-changing technology, the Committee concluded that an ongoing engagement with that evolving technology in the form of security issues to consider and reconsider was preferable to a “bright line” or categorical approach.

This opinion extends that analysis to a broad range of cyber risks associated with the use of electronic devices and systems that contain confidential client information and connect to the internet and, thus, are theoretically accessible to anyone with an internet connection.

STATEMENT OF FACTS

Attorney A

Attorney A’s laptop is stolen. Attorney A did not store confidential client information on the laptop, but only used the laptop to access such information remotely. Also, the laptop could not be accessed without biometric authentication. Attorney A’s law firm also installed software on the laptop that allowed it to be remotely locked down and erased. As soon as Attorney A realizes that the laptop has been stolen, Attorney A contacts law firm’s IT department and receives confirmation almost immediately that the laptop has been located, locked down, and wiped clean.

Attorney B

At the end of a busy day, Attorney B realizes that Attorney has lost Attorney’s smartphone. Attorney B regularly uses the smartphone to email and text clients and to access certain practice management software applications related to clients. The smartphone is only protected by a 4-character password and not any biometric security system. Attorney B does not have any software installed on the smartphone that allows it to be remotely tracked, locked down, and/or wiped clean.

Before going to bed, Attorney B remembers that Attorney left the smartphone in a tote bag at the restaurant where Attorney had dinner with a friend. Attorney B immediately calls the restaurant, but it is closed. Attorney B goes to the restaurant when it opens the next morning and retrieves Attorney’s bag and smartphone which, the manager tells Attorney, was locked in a cabinet overnight. Nothing appears to be missing and the smartphone is still in the pocket of the bag where Attorney had left it.

Law Firm C

Law Firm C is a four member firm specializing in corporate law. Law Firm’s receptionist routinely receives emails sent to the firm (rather than to a specific attorney or staff member) and routes them to the appropriate person. Just before the end of the business day, the

receptionist receives an email from a business purporting to be Law Firm's IT provider. The email looked entirely genuine and asked the receptionist to click on the attachment to allow the firm to do routine maintenance on Law Firm's server. Receptionist did so which resulted in ransomware being installed on Law Firm's network, immediately locking up the Law Firm's computers, and displaying a message demanding that a sum of money be transferred electronically by cryptocurrency to unlock Law Firm's computers. Law Firm C pays the ransom and regains access to its data. In consultation with security experts, Law Firm C determines that no client information was accessed and none of the matters being handled by Law Firm are negatively impacted by the delay.

Attorney D

Attorney D is outside counsel for a life sciences technology company ("Company") for whom Attorney has been working on obtaining several very important patents. While on vacation, Attorney D goes to a coffee shop to check personal and work emails. Attorney D's laptop is not encrypted. Instead of using a virtual private network or personal hotspot to connect to the internet, Attorney accesses the shop's public Wi-Fi network. Unknown to patrons or coffee shop staff, a hacker has set up a fake internet portal that resembles the one provided by the coffee shop. Attorney D does not realize that Attorney actually logged on to that fake Wi-Fi network.

Attorney D returns to the same coffee shop the next day and notices a sign warning patrons about the fake Wi-Fi. After returning to the office the following week, Attorney D has the law firm's technology team examine the laptop. The technology team concludes that someone had accessed certain files on the laptop related to Company's patents while Attorney D was connected to the fake Wi-Fi network. Since Attorney D did not review those files on that day, it appears reasonably likely that an unauthorized user had done so.

DISCUSSION

A. Duty of Competence and Confidentiality

The duty of competence (rule 1.1) and the duty to safeguard clients' confidences and secrets (rule 1.6 and Bus. & Prof. Code, § 6068(e)) require lawyers to make reasonable efforts to protect such information from unauthorized disclosure or destruction. The threshold requirement is for lawyers to have a basic understanding of the "benefits and risks associated with relevant technology." Cal. State Bar Formal Opn. No. 2015-193; see also Comment [8] to ABA Model Rule 1.1.^{3/} This general principle requires lawyers to have a basic understanding of

^{3/} Although the California rules do not include a Comment similar to Comment [8] of ABA Model Rule 1.1, the Committee cited to that Comment in support of the Committee's analysis in Formal Opn. 2015-193. At the time this opinion was published, the Board of Trustees has adopted for submission to the California Supreme Court for approval, a new Comment [1] to rule 1.1 which states: "The duties set forth

the risks posed when using a given technology and, if necessary, obtain help from appropriate technology experts on assessing those risks and taking reasonable steps to prevent data breaches which potentially can harm clients.^{4/} The threshold obligation to understand the risks is satisfied by learning where and how confidential client information is vulnerable to unauthorized access. This inquiry must be made with respect to each type of electronic device or system as they have been or are incorporated into the lawyer's practice.

For example, computer systems can be breached by inadvertently clicking on a link in a seemingly legitimate "phishing" email or text message or by installing an unvetted software application which can install malicious software on the system. Portable electronic devices can be accessed if security precautions, such as passwords, are disabled or inadequate. Data on a laptop computer can be accessed if the laptop is connected to a public or other inadequately secured network and if the data is not properly protected. And the threats vary and widen as data thieves develop their attack strategies and as technologies develop. Thus, lawyers must understand how their particular use of electronic devices and systems pose risks of unauthorized access, they must be knowledgeable about the options available at any given point in time to minimize those risks (including how best to store or control access to said information), and they then must implement reasonable security measures in light of the risks posed. In addition, because law firms are frequent targets, law firms should consider whether rule 5.1 requires law firms to prepare a data breach response plan so that all stakeholders know how to respond when a breach occurs.^{5/}

ABA Formal Opn. No. 18-483 (Lawyer's Obligations After an Electronic Data Breach or Cyberattack) provides a useful list of competence-based duties that explain the requirement of "reasonable efforts" in addressing the potential for inadvertent disclosure of confidential client information due to a data breach:

- The obligation to monitor for a data breach: "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 and the use of data." *Id.* at p. 5.

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."

^{4/} This Committee recognizes that while lawyers are not required to become technology experts and master the complexities and deficiencies of the security features of each technology available, lawyers owe clients a duty to have a basic understanding of the protections afforded by the technology used in their practice. If a lawyer lacks the necessary competence to assess the security of the technology, the lawyer must seek additional information, or consult with someone who possesses the necessary knowledge, such as an information technology consultant. (Cal. State Bar Formal Opn. Nos. 2012-184, 2010-179.)

^{5/} ABA Formal Opn. No. 18-483 at pp. 6-7, and the ABA Cybersecurity Handbook, identify various considerations in developing a data breach response plan.

- When a breach is detected or suspected, lawyers must “act reasonably and promptly to stop the breach and mitigate damage resulting from the breach.” *Id.* at p. 6. A preferable approach is to have a data breach plan in place “that will allow the firm to promptly respond in a coordinated manner to any type of security incident or cyber intrusion.” *Id.* at p. 6.
- Investigate and determine what happened: “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.” *Id.* at p. 7.

The duty to make reasonable efforts to preserve confidential client information does not create a strict liability standard nor does the duty “require the lawyer to be invulnerable or impenetrable.” ABA Formal Opn. No. 18-483 at p. 9. The precise nature of the security measures that attorneys are expected to take depends on the circumstances. But, as the ABA has noted, “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.” *Id.* (quoting from the 2017 ABA Cybersecurity Handbook at p. 73).

“Reasonable efforts” are those which are reasonably calculated under the circumstances to minimize particular identified risks. For example, when law firm personnel work on client matters remotely, the law firm must ensure that all data flowing to and from those remote locations and the firm’s servers or cloud storage is adequately secured. The particular method or methods selected (VPN, encryption, etc.) will reflect the firm’s due consideration of the risks, the relative ease of use of different security precautions, time that would have to be spent training staff, and the like. Some security precautions are so readily available and user-friendly (such as the ability to locate and lock down portable devices in the event of loss or theft), that failure to implement them could be deemed unreasonable. Others will require a deeper assessment.

Finally, in law firms with subordinate lawyers, the lawyers with management or supervisory responsibilities should be aware of their obligations under rules 5.1 and 5.3. Rule 5.1(a) requires lawyers with “managerial authority in a law firm [to] make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that all lawyers in the firm comply with these rules and the State Bar Act.” Thus, lawyers with managerial authority within a law firm must make a reasonable effort to establish internal policies and procedures designed to protect confidential client information from the risk of inadvertent disclosure and data breaches as a result of technology use, which includes monitoring the use of technology and office resources connected to the internet and external data sources. ABA Formal Opn. No.

18-483. The law firm should also consider whether they are required to proactively establish protocols for responding to and addressing potential data breaches. Rule 5.1(b) requires supervisory attorneys to ensure that subordinate attorneys within the firm comply with the rules and policies and procedures established by the firm. And rule 5.3 makes these principles applicable to non-lawyer staff.

Thus, part of the risk assessment process should include reasonable efforts to ensure that all firm members appreciate the risks involved in keeping confidential client information on electronic systems and the steps that the firm's managers have implemented to minimize the risk of unauthorized disclosure. Because the risk-assessment process is on-going, particularly with the introduction of new technologies and new threats, this duty would require managers and supervisors to establish ongoing and evolving protective measures with respect to the use of its technology, and regularly monitoring the same, and to keep subordinate lawyers and staff up to date as new measures are implemented.

However, under rule 5.2, subordinate lawyers have independent ethical obligations to protect confidential client information as part of their duty of competence. Thus, subordinate lawyers should not blindly follow firm technological rules that are unreasonable or rely on the absence of a firm rule where there should be one. See Comment to rule 5.2.

B. Duty of Disclosure

Rule 1.4(a)(3) and Business and Professions Code section 6068(m) require attorneys to keep their clients^{6/} "reasonably informed about significant developments" relating to the attorney's representation of the client. Neither rule nor case law define what events qualify as "significant." (See, e.g., Tuft et al., *Cal. Practice Guide: Professional Responsibility* (The Rutter Group 2018) Ch. 6-B, § 6:128, acknowledging that what is "significant" under these provisions varies with each client's needs and the nature of the representation.) Nevertheless, the relevant authorities have uniformly concluded that the misappropriation, destruction, or compromising of confidential client information, or a cyber breach that has significantly impaired the lawyer's ability to provide legal services to clients, is a "significant development" that must be communicated to the client. See, e.g., ABA Formal Opn. No. 18-483 at p. 10; New

^{6/} This opinion focuses on current clients and does not address the duty of disclosure owed to former clients. For discussion concerning a lawyer's duty to notify a former client of a data breach, compare ABA Formal Opn. No. 18-483 at pp. 13-14 (declining to impose a duty to notify a former client under the Model Rules of Professional Conduct, while noting that data privacy laws, common law duties of care and contractual arrangements with clients may give rise to such a duty) and Maine Professional Ethics Commission Opinion No. 220 "Cyberattack and Data Breach: The Ethics of Prevention and Response" issued on April 11, 2019 (opining, based on its interpretation of Maine's Rules of Professional Conduct, Rule 1.9, that "a former client is entitled to no less protection and candor than a current client in the case of compromised secrets and confidences. A former client must be timely notified regarding a cyberattack or data breach that has, or may have, exposed the client's confidences or secrets.")

York State Bar Association Ethics Opn. No. 842 (2010) (involving a data breach of a cloud storage provider); ABA Formal Opn. No. 95-398.

ABA Formal Opn. No. 18-483 describes a “data breach” as 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.” ABA 18-483 at p. 4.^{7/} Thus, not all events involving lost or stolen devices, or unauthorized access to technology, would necessarily be considered a data breach. Consistent with their obligation to investigate a potential data breach, however, lawyers and law firms should undertake reasonable efforts, likely through the use of individuals with expertise in such investigations, to ascertain, among other things, the identity of the clients affected, the amount and sensitivity of the client information involved, and the likelihood that the information has been or will be misused to the client’s disadvantage. This will assist in determining whether there is a duty to disclose. If the lawyer or law firm is unable to make such a determination, the client should be advised on that fact. *Id.* at p. 14.

Lawyers and clients may also differ as to what events would trigger the duty to disclose. The key principle, however, in considering whether the event rises to the level of a data breach, is whether the client’s interests have a “reasonable possibility of being negatively impacted.” ABA 18-483 at p. 11. Certainly disclosure is required in situations where a client will have to make decisions relevant to the breach, such as the need to take mitigating steps to prevent or minimize the harm, or to analyze how the client’s matter should be handled going forward in light of a breach. When in doubt, lawyers should assume that their clients would want to know and should err on the side of disclosure.

C. If Disclosure to Clients is Required, When and What Must be Disclosed?

In all cases involving a data breach, disclosure to clients must be made as soon as reasonably possible so that the affected clients can take steps to ameliorate the harm.^{8/} For example, affected clients might want or need to change passwords and modify or delete online accounts. However, it may be reasonable for the lawyer, through the use of a security expert, to attempt to ascertain the nature and extent of the potential breach prior to communicating this information to the client. The more that is known related to the breach, including exactly what information might have been accessed, the better the response plan. Given the obligation to preserve client confidences, secrets and propriety information, it is appropriate to assume that

^{7/} The Committee believes this description is useful in understanding what constitutes a data breach for the purpose of this opinion and discussion, and has adopted the same approach here.

^{8/} Lawyers and law firms should also consider notifying insurance carriers as soon as possible of any circumstances giving rise to a potential breach to put the carrier on notice. While typically such acts are only covered by specific Cyber Coverage policies, not Lawyer’s Professional Liability (LPL) or Commercial General Liability (CGL) policies, these policies typically have fairly short time limits within which notice must be given.

reasonable clients would want to be notified if any of that information was acquired or reasonably suspected of being acquired by unauthorized persons.

With respect to the details of a required disclosure, the attorney “shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions” as to what to do next, if anything. (Rule 1.4(b)). “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 its 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.” ABA 18-483 at p. 14.

Lawyers may also have notification obligations under Civil Code section 1798.82 and federal and international laws and regulations such as HIPAA and the EU General Data Protection Regulation.

D. The Factual Scenarios

Although Attorney A’s laptop is stolen and it could be used to access confidential client information, the risk of unauthorized access to such information was mitigated by Attorney A and law firm’s policies for addressing these types of cyber risks. First, Attorney A did not store confidential client information on the laptop, but only used the laptop to access such information remotely. Second, Attorney A had a biometric security system on the laptop reducing the chances that it could be hacked by an unauthorized user. Third, Attorney A’s law firm had the ability to quickly and easily locate, lock, and wipe clean the laptop, almost guaranteeing that there was no unauthorized access to any confidential client information. Under these facts, where there is no evidence of unauthorized access or harm, Attorney A would not have a duty to disclose to any client the fact that Attorney lost the laptop.

Attorney B’s temporary loss of a smartphone, under these circumstances, is unlikely to be considered a data breach, particularly if Attorney B can obtain assurances from the restaurant owner/staff that only the restaurant had access to it and that no one accessed the phone’s contents after Attorney B left. Because it does not appear that the data on Attorney B’s phone was misappropriated, destroyed, or compromised, the temporary loss of the phone is unlikely to constitute a significant development and no duty to disclose would likely be triggered.

Under these circumstances, however, Attorney B and Attorney B’s law firm should consider whether it should require all law firm attorneys to have stronger passwords, or use biometric security systems on firm issued smartphones, or if the law firm should prohibit their attorneys from accessing client data, including emails, on the attorneys’ personal smartphones. The firm should also consider requiring all smart phones used for firm matters to have software installed to locate, lock, and wipe devices if they are lost or stolen, and specific protocols for managing such scenarios. Next time, Attorney B may not be so confident in Attorney’s assessment that no client data was accessed, particularly if the phone is one day stolen. For example, it is possible that Attorney B’s cell phone provider could have locked down the phone remotely, but Attorney B did not consider this option or look to the law firm for advice on handling this

situation. Finally, when electronic devices are temporarily lost or misplaced, the law firm should consider whether its policies should include requiring its IT team to examine those devices once the device is recovered in order to determine whether any unauthorized access took place.

The situation of Law Firm C involves a common entry point for hackers: malware attached to a seemingly legitimate email, also referred to as “phishing.” Given the ubiquity of this method of gaining access, solo practitioners and firms must consider implementing reasonable precautions, such as staff and attorney trainings warning of this risk and protocols for handling incoming emails. Law Firm C has certainly been inconvenienced by the cyber breach, but the firm has confirmed that none of its clients were actually or potentially harmed because no confidential client information was accessed, and the short delay did not impair the firm’s attorneys from continuing to provide necessary legal services to its clients. Therefore, the firm would not be required to disclose the incident. On the other hand, if the consultant could not preclude actual or potential unauthorized access, a risk of client harm remains and disclosure would be required.

Attorneys who keep confidential information on their devices ought to be aware that accessing public Wi-Fi or other unsecure networks may open another access point for hackers. This is illustrated by Attorney D’s exposing confidential information to anyone with the ability to electronically “eavesdrop” on the Attorney’s keystrokes. Attorneys who work on client matters remotely must consider the risks of harm and take reasonable precautions, as discussed above, to prevent unauthorized disclosure. Cal. State Bar Formal Opn. No. 2010-179 at p. 6 (discussing the use of a laptop in unsecured and secured settings). Attorney D’s failure to secure their online communications exposed confidential information to a hacker and it is unknown if, or to what extent, the hacker would or could use such information. It is this Committee’s view that Attorney D risked violating the duties of confidentiality and competence by using a public wireless connection without taking appropriate precautions, such as the use of encryption, a VPN or other protective measures. (Cal. State Bar Formal Opn. No. 2010-179.)

Since the law firm was able to confirm the unauthorized access of confidential client information, Attorney D and the law firm must notify the client, Company, as soon as possible. Although it is unknown if or how the hacker might use the information, because of the sensitive nature of the information to Company’s business, the misappropriation would constitute a significant development and require appropriate notice to the client. “[D]isclosure will be required if material client information was actually or reasonably suspected to have been accessed, disclosed or lost in a breach.” ABA 18-483 at p. 14.

Once a disclosure is made, Attorney D and the law firm can evaluate with Company the likelihood that the information will be used by the hacker and may decide to speed up the timeline for obtaining the relevant patents related to the information that was inadvertently disclosed to mitigate potential harm.^{9/} Of course, the event would also require Attorney D and the law

^{9/} In addition, because Attorney D’s handling of confidential client information may constitute an error giving rise to a potential malpractice claim, Attorney D and law firm should also consider whether a

firm to take appropriate remedial steps in terms of evaluating the firm's policies related to attorney's accessing firm devices from unsecured locations. It should also consider reinforcing policies requiring attorneys to promptly address any irregularities or suspicions related to potential data breaches with the firm's technology officers as soon as they are discovered.

CONCLUSION

The use of computers and portable electronic devices by lawyers is now ubiquitous and has increased the risk of client confidential client information being accessed by unauthorized users. Lawyers must assess the risks involved in the use of electronic devices and systems that contain, or access, confidential client information and to take reasonable precautions to ensure that that information remains secure. This duty extends to law firms whose managers must make a reasonable effort to establish internal policies and procedures designed to protect confidential client information from the risk of inadvertent disclosure and data breaches as a result of technology use, to monitor such use, and to stay abreast of current trends and risks. The creation of a data breach response plan may also be required to identify the risks posed to the firm's then-current use of technology and feasible precautions.

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.

conflict of interest has arisen between the law firm and client such that the law firm should also comply with rule 1.7 in disclosing this significant development to client. (See also Cal. State Bar Formal Opn. No. 2019-197).



Los Angeles County Bar Association

1055 West 7th Street, Suite 2700 | Los Angeles, CA 90017-2553

Telephone: 213.627.2727 | www.lacba.org

June 15, 2020

Angela Marlaud
Office of Professional Competence,
Mandatory Fee Arbitration Program
State Bar of California
180 Howard Street
San Francisco, CA 94105

Re: Interim Opinion 16-0002 (revised)

Dear Angela:

The Professional Responsibility and Ethics Committee of the Los Angeles County Bar Association appreciates the opportunity to submit the following comments on the revised draft of proposed Interim Opinion No. 16-0002.

While we continue to agree with much of the proposed opinion, we do have these comments and suggestions:

1) We said about the initial public comment draft that the use of “minimize” is not correct, but the revised draft does not fix this important error. As an example, the Digest in both drafts says that a lawyer’s duty is “to minimize the risk of unauthorized access.” (emphasis added). The word “minimize” means “**reduce** (something, especially something unwanted or unpleasant) **to the smallest possible amount or degree.**” This is not and never has been a disciplinary standard. No lawyer is subject to discipline, and no lawyer should suffer the costs and other consequences of a disciplinary threat, merely because someone better informed, more clever, or with deeper pockets could have done something more. The language of rule 1.1 makes this clear. Because advisory ethics opinions are referenced in civil matters, it also is important that perfection also is not a civil standard. As a famous judge put it: “Legal malpractice is not a failure to be brilliant” *McKnight v. Dean*, 270 F.3d 513, 518 (7th Cir. 2001) (Posner, J.) The term “minimize” is used several times in the current draft, and the same standard is expressed in other ways. For example, “how best to store or control access” is found near the top of p. 4. This aspect of the draft is fundamentally wrong, and in addition it is inconsistent with the draft’s simultaneous use of “reasonable” and “reasonably.” For example,

“reasonable” appears three times in the Digest. The correct statement is that a lawyer is obligated to act competently to “reduce” the risk of unauthorized access, just as lawyers are with the handling of their paper files (in file rooms, on desks and conference tables, and in brief cases), snail mail and telephonic communications, and in sending telegrams in earlier days. Any reference to a standard of perfection also would conflict with prior advisory opinions. See, e.g., Cal. State Bar Formal Op. 1997-150, a pre-internet opinion, which has this Digest: “Attorneys sharing space or staff must take reasonable steps under the circumstances to ensure that their clients and potential clients are not deceived, misled or confused regarding the nature of their relationship. Attorneys who share office space or services also must take reasonable steps under the circumstances to protect each client’s confidence and secrets. If attorneys do not address these issues sufficiently, they may violate their obligation to maintain clients’ confidential information.” Any suggestion that a lawyer’s duty to maintain the confidentiality of client secrets goes beyond a standard of reasonableness also would be inconsistent at least with Cal. State Bar Formal Op. 2010-179 and L.A. County Bar Formal Op. 529 (2017).

2) The second sentence of the second Introduction paragraph can be made more accurate by replacing the phrase “... arising from accessing client confidential information...” with: “... that arise when a lawyer accesses confidential client information” The reason for this change is that the lawyer’s duty is limited to the lawyer’s own actions and not the actions of any other person, such as the client, when accessing the client’s own confidential information.

3) We recommend removing the second sentence in footnote 3. A proposed rule Comment has no instructive authority. It remains to be seen whether the proposed Comment will be adopted, and in what form if it is.

4) The first sentence is inconsistent in number. It should be: “lawyers are not required to become technology experts” There is a word missing and another inconsistency in number later in that sentence (“used [in] their practices.”).

5) The last full sentence on p. 3 has another inconsistency in number: “Data on a laptop computer can be accessed if the laptop ...”

Thank you for the opportunity to comment on the Proposed Formal Opinion.

Sincerely,



Brandon Niles Krueger
Chair
Professional Responsibility and Ethics Committee,
Los Angeles County Bar Association



**ORANGE COUNTY
BAR ASSOCIATION**

PRESIDENT

SCOTT B. GARNER

PRESIDENT-ELECT

LARISA M. DINSMOOR

TREASURER

DANIEL S. ROBINSON

SECRETARY

MICHAEL A. GREGG

IMMEDIATE PAST PRESIDENT

DEIRDRE M. KELLY

DIRECTORS

ALEXANDER W. AVERY

ANTOINETTE N. BALTA

JOHN K. BECKLEY

KATE CORRIGAN

SHIRIN FOROOTAN

KELLY L. GALLIGAN

JOHN S. GIBSON

JOSH JI

MICHAEL S. LEBOFF

ADRIANNE E. MARSHACK

TERESA A. MCQUEEN

TRACY A. MILLER

JAMES Y. PACK

MELISSA A. PETROFSKY

THOMAS A. PISTONE

MARY-CHRISTINE SUNGAILA

YOLANDA V. TORRES

MEI TSANG

DARRELL P. WHITE

CHRISTINA M. ZABAT-FRAN

ABA REPRESENTATIVE

RICHARD W. MILLAR, JR.

CEO/EXECUTIVE DIRECTOR

TRUDY C. LEVINDOFSKE

AFFILIATE BARS

ASSOC. OF BUSINESS TRIAL LAWYERS,

OC CHAPTER

CELTIC BAR ASSOC.

FEDERAL BAR ASSOC.,

OC CHAPTER

HISPANIC BAR ASSOC. OF OC

IRANIAN AMERICAN BAR ASSOC.,

OC CHAPTER

ITALIAN AMERICAN LAWYERS

OF OC – LEX ROMANA

J. REUBEN CLARK LAW SOCIETY

OC ASIAN AMERICAN BAR ASSOC.

OC CRIMINAL DEFENSE BAR ASSOC.

OC JEWISH BAR ASSOC.

OC KOREAN AMERICAN BAR ASSOC.

OC LAVENDER BAR ASSOC.

OC TRIAL LAWYERS ASSOC.

OC WOMEN LAWYERS ASSOC.

THURGOOD MARSHALL BAR ASSOC.

P.O. BOX 6130

NEWPORT BEACH, CA 92658

TELEPHONE 949/440-6700

FACSIMILE 949/440-6710

WWW.OCBAR.ORG

June 24, 2020

Angela Marlaud

Office of Professional Competence, Planning and Development

State Bar of California

180 Howard Street

San Francisco, California 94105-1639

Via Email: angela.marlaud@calbar.ca.gov

Re: Proposed Formal Opinion No. 16-0002

Dear Ms. Marlaud:

The Orange County Bar Association (OCBA) respectfully submits the following comments concerning Proposed Formal Opinion No. 16-0002.

Founded over 100 Years ago, the OCBA has approximately 7,500 members, making it one of the largest voluntary bar associations in California. The OCBA Board of Directors made up of practitioners from large and small firms, with varied civil and criminal practices, of different ethnic backgrounds and political learnings, has approved these comments prepared by the Professionalism and Ethics Committee.

We believe that the opinion provides valuable guidance. At the same time, we have comments and suggestions that we believe could clarify, strengthen, and improve the opinion and provide even more clarity for practitioners confronted with these dilemmas, which we address below.

While we appreciate that COPRAC has endeavored in this draft of Proposed Opinion 16-0002 to address the issue more directly, we are concerned about the opinion's conclusion that lawyers do not have a duty to disclose a data breach to former clients in all circumstances. In particular, footnote 6 of Proposed Formal Opinion No. 16-0002:

“This opinion focuses on current clients and does not address the duty of disclosure owed to former clients. The Committee agrees with the discussion of this issue in ABA Formal Opn. No. 18-483, and does not believe that California’s rule 1.9 imposes a duty to notify a former client of a data breach, although other applicable law may require notification. See ABA Formal Opn. No. 18-483 at p. 13 - 14.”

However, we believe that, even though disclosure may not be required by rule 1.9, other ethical obligations or rules may be implicated that could require

disclosure to a former client, at least where the former client's confidential information was, or was reasonably likely, revealed in the data breach. We would encourage the committee to re-consider its conclusion and perhaps adopt a more nuanced approach, in light of the following:

1. ABA Opinion 18-483's commentary, including some or all of the following, demonstrates that its reasoning and conclusions may have limited application:

a. The ABA's conclusion was based on rule 1.9(c)'s prohibition on revealing a former client's information, but acknowledged that the rule does not describe what steps, if any, a lawyer should take if such information is revealed. Thus, we question whether rule 1.9 defines a lawyer's duties to a former client when confidential information is revealed.

b. The ABA states that 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 the former client relating to records retention, may mandate notice to former clients of a data breach. Although Footnote 6 of 16-0002 acknowledges that other laws may require notification, we believe it would helpful to spell out which ones.

c. The ABA states that, 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. It is probably worth noting this comment in footnote 6.

2. At least one other ethics committee has come to a conclusion on this point contrary to ABA 18-483, That opinion merits consideration and, at a minimum, mention in 16-0002. Specifically, the Maine Professional Ethics Commission Opinion #220 "Cyberattack and Data Breach: The Ethics of Prevention and Response" issued on April 11, 2019 (the "Maine Opinion") concluded:

"[a] former client must be timely notified regarding a cyberattack or data breach that has, or may have, exposed the client's confidences or secrets."

In so concluding, the Maine Commission also focused on rule 1.9. Maine rule 1.9 provides that a lawyer shall not reveal confidences or secrets of a former client except as the Rules would permit or require with respect to a current client. The duty of confidentiality survives the termination of the client-lawyer relationship and trust is the “hallmark of the client-lawyer relationship” whether for a current or a former client. California’s articulation of rule 1.9 contains similar language. Based on this, the Maine Commission concluded that a former client is entitled to no less protection and candor than a current client in the case of compromised secrets and confidences. A former client must be timely notified regarding a cyberattack or data breach that has, or may have, exposed the client’s confidences or secrets.

Thank you for your consideration of our comments and suggestions.

Sincerely,

A handwritten signature in black ink, appearing to read 'S.B. Garner', with a long horizontal flourish extending to the right.

Scott B. Garner
2020 President
Orange County Bar Association

Re: Proposed Formal Opinion No. 16-0002

June 24, 2020

Page | 4

Marlaud, Angela

From: form_engine@fs16.formsite.com on behalf of Formsite <form_engine@fs16.formsite.com>
Sent: Tuesday, May 05, 2020 10:09 AM
To: Marlaud, Angela
Subject: 16-0002 - Public Comment Form Result #13003944

Commenting on behalf of an organization No

Name Mina Sirkin

City Woodland Hills

State California

Email address minasirkin@gmail.com

From the choices below, we ask that you indicate your position. (This is a required field.) Oppose

ENTER COMMENTS HERE. To upload files proceed to the ATTACHMENTS section below.

That puts a large burden on lawyers which may not be accomplishable by small firms. For example, if the State Bar accidentally sent an email regarding the Bar questions, that impact cannot be undone once sent. Once a breach occurs, and data has been compromised, there is very little a lawyer can do. The best thing is to just disclose the use of cloud technology and explain its risks at the time client retains them. This is just like logging into an app with an agreement that the use of cloud technology has risks.

This email was sent to angela.marlaud@calbar.ca.gov as a result of a form being completed.
[Click here](#) to report unwanted email.

From: form_engine@fs16.formsite.com on behalf of [Formsite](#)
To: [Marlaud, Angela](#)
Subject: 16-0002 - Public Comment Form Result #13149742
Date: Tuesday, June 23, 2020 10:24:59 AM

Commenting on behalf of an organization No

Name Felicia Cansada Williams

City Campbell

State California

Email address FeliciaWilliamsGullatt04@gmail.com

From the choices below, we ask that you indicate your position. (This is a required field.) Support

ENTER COMMENTS HERE. To upload files proceed to the ATTACHMENTS section below.

As a former employee of the District Attorney's Office (City & County of San Francisco), I was forced into early retirement duty to a agency-wide "data breach." According to Federal Law, medical history is only released upon a signed authorization of the client in question.

I was given a retirement w h ending I requested leave of absence due to poor working conditions, respiratory problems, and Carol tunnel syndrome which was recommended by my primary care physician at Kaiser Permanente Medical Group in San Francisco. I worked weekends for two years, August through November, to retire and seal juvenile records. Upon recommendations from the Office Manager, Martha Knudsen, my position was upgraded to Class 8132 Investigative Assistant.

Please note: I had been working out of my classification for approximately 4 years. However, rumors spread rapidly that I was mentally ill by Assistant District Attorneys as well as Legal Secretaries. I was not allowed to compete for subsequent positions, enter the premises of the Youth Guidance Center, nor was I able to speak with Human Resources Management staff, via telephone or in person.

It has been a traumatic experience to my household to endure homelessness for 10 years now due to an erroneous "data breach." I also appealed the decision of not receiving Disability Retirement; however, it was seven (7) years before I was approved for Social Security Disability Insurance benefits.

I acquired an AAS Degree. as a Paralegal Specialist, graduated with honors (Phi Theta Kappa) in 2012. To date, no one from SFDA will generate a Letter of Employment Verification. I have even connected and communicated with Senator Kamala D. Harris, my late Department Head/superior, without success. Finally, it is my opinion that San Francisco should be held accountable, in addition to the State of California.

Great damages. A TORT.

This email was sent to angela.marlaud@calbar.ca.gov as a result of a form being completed.
[Click here](#) to report unwanted email.