

**HEADLINE: Proposed Formal Opinion Interim No. 16-0002 (Data Breaches)**

**SUBHEAD: The State Bar seeks public comment on Proposed Formal Opinion Interim No. 16-0002 (Data Breaches).**

**Deadline: March 30, 2020**

**Background**

The State Bar Standing Committee on Professional Responsibility and Conduct (COPRAC) is charged with the task of issuing advisory opinions on the ethical propriety of hypothetical attorney conduct. In accordance with State Bar policy and procedure, the Committee shall publish proposed formal opinions for public comment (See, State Bar Board of Trustee Resolutions July 1979 and December 2004. See also, Board of Trustee Resolution November 2016).

On May 10, 2018, the California Supreme Court issued [an order](#) approving 69 new Rules of Professional Conduct, which will go into effect on November 1, 2018. Information about the new rules is available at the [State Bar website](#). Proposed Formal Opinion Interim No. 16-0002 interprets the new Rules of Professional Conduct.

**Discussion/Proposal**

Proposed Formal Opinion Interim No. 16-0002 considers: What are a lawyer's ethical obligations with respect to unauthorized access by third persons to electronically stored client confidential information in the lawyer's possession?

The opinion interprets 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; Business and Professions Code sections 6068(e) and 6068(m); and Civil Code section 1798.82.

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.

At its December 6, 2019 meeting and in accordance with its Rules of Procedure, the State Bar Standing Committee on Professional Responsibility and Conduct tentatively approved Proposed Formal Opinion Interim No. 16-0002 for a 90-day public comment distribution.

**Any fiscal/personnel impact**

None

**Background material**

Proposed Formal Opinion Interim No. 16-0002

**Source**

State Bar Standing Committee on Professional Responsibility and Conduct

**Deadline**

March 30, 2020

**Direct comments to**

Angela Marlaud  
Office of Professional Competence  
State Bar of California  
180 Howard Street  
San Francisco, CA 94105-1639  
Ph. # (415) 538-2116  
Fax # (415) 538-2171  
E-mail: [angela.marlaud@calbar.ca.gov](mailto:angela.marlaud@calbar.ca.gov)

**THE STATE BAR OF CALIFORNIA  
STANDING COMMITTEE ON  
PROFESSIONAL RESPONSIBILITY AND CONDUCT  
FORMAL OPINION INTERIM NO. 16-0002**

**ISSUE:** What are a lawyer’s ethical obligations with respect to unauthorized access by third persons to electronically stored client confidential 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.<sup>1</sup>

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 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 (“COPRAC” or “Committee”) discussed lawyers’ ethical obligations when dealing with e-discovery. In Cal. State Bar Formal Opn. No. 2010-179, the Committee discussed ethical issues arising from accessing client confidential information on a laptop over public Wi-Fi and 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 competency and confidentiality.

---

<sup>1</sup> Unless otherwise indicated, all references to “rules” in this opinion will be to the Rules of Professional Conduct of the State Bar of California.

In light of ever changing technology, the Committee concludes that an on-going engagement with that evolving technology in the form of security issues to consider and re-consider 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 client confidential 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 realized 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 protected only by a 4-character password and not any biometric data. 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 e-mails sent to the firm (rather than to a specific attorney or staff member) and routes them to the appropriate person. Just before quitting time, the receptionist received an e-mail from a business purporting to be Law Firm’s IT provider; it 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 and ransomware installed itself on Law Firm’s network, immediately locked up the Law Firm’s computers, and displayed a message

demanding that a sum of money be transferred electronically by cryptocurrency to unlock Law Firm's computers. Law Firm C paid the ransom and regained access to its data. In consultation with security experts, Law Firm C determined that no client information was accessed and none of the matters being handled by Law Firm were 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. On vacation, Attorney D goes to a coffee shop to check personal and work e-mails. Attorney D's laptop was 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 had set up a fake internet portal that resembled the one provided by the coffee shop. Attorney D doesn't realize that Attorney actually logged on to that fake network.

Attorney D returned to the same coffee shop the next day and noticed a sign warning patrons about the fake internet portal. Upon return to the office the following week, Attorney D had the law firm's technology team examine the laptop. The technology team concluded that someone had accessed certain files on the laptop related to Company's patents while Attorney D had been on the fake internet network. Since Attorney D was not reviewing those files on that day, it appeared reasonably likely that an unauthorized user had done so.

## **DISCUSSION**

### **Confidentiality and Competency**

The duty of competency (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. This general principle requires lawyers to have a basic understanding of 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. The threshold obligation to understand the risks is satisfied by learning where and how confidential 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" e-mail 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 missing or inadequate. Data on laptop computers 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 preparing a data breach response plan so that all stakeholders know how to respond when a breach occurs.<sup>2</sup>

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.
- 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 client confidential 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 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

---

<sup>2</sup> Discussed in ABA Formal Opn. No. 18-483 at pp. 6-7 and in the ABA Cybersecurity Handbook.

updated in response to new developments.” *Id.* (quoting from the ABA Cybersecurity Handbook at p. 73).

“Reasonable efforts” are those which are reasonably calculated to eliminate, or at least minimize, particular, identified risks. For example, if a firm allows its staff to work on client matters remotely, it 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 the 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 proactively establishing 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.

### **Duty of Disclosure**

Rule 1.4(a)(3) and Business and Professions Code section 6068(m) require attorneys to keep their clients<sup>3</sup> “reasonably informed about significant developments” relating to the attorney’s representation of the client. Neither rule nor case law clearly define what events qualify as

---

<sup>3</sup> This opinion focuses on current clients and does not address the duty of disclosure owed to former clients. See discussion of this in ABA 18-483 at p. 13-14.

“significant.” (See, e.g., Tuft et al., *Cal. Practice Guide: Professional Responsibility* (The Rutter Group 2018) § 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 client confidential 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 10; New 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.<sup>4</sup> 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 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.

### **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 the affected clients can take steps to ameliorate the harm.<sup>5</sup> For example, affected clients might want or need to change passwords and modify or delete on-line accounts.

---

<sup>4</sup> 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.

<sup>5</sup> 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. Policies typically have fairly short time limits within which notice must be given.

However, it is certainly reasonable for the lawyer, through the use of a security expert, to attempt 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 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 HIPPA and the EU General Data Protection Regulation.

### **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 password 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 law firm should consider whether it should require all law firm attorneys to have stronger passwords, or ones that use biometric data, on firm issued smart phones or if law firm should allow their attorneys to access client data, including emails, on the attorney’s 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. 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. 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 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 e-mail, 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 training warning of this risk and protocols for handling in-coming e-mails. 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 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 portable 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 capability of electronically "eavesdropping" 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 use of laptop in unsecured and secured settings). Attorney D's failure to secure their on-line communications exposed confidential information to a hacker and it is unknown if, or to what extent, the hacker would or could use such information.

Since the law firm was able to confirm the unauthorized access of confidential client information, Attorney D and 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 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. Of course, the event would also require Attorney D and law 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 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 is also recommended 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.

**Lee, Mimi**

---

**From:** Carol M Langford <langford@usfca.edu>  
**Sent:** Thursday, January 02, 2020 3:30 PM  
**To:** Difuntorum, Randall; Tuft, Andrew  
**Subject:** Proposed Opinion 16-0002

Once again the Committee is giving us an opinion that has great practical use. The COPRAC people are on fire! The only thing I would change is the part about supervisory authority. That part is tough, as there are lawyers practising as solos with secretaries; and small, medium and large firms. In large firms monitoring how employees and non-employees use the internet is harder.

Also, it needs to say that each state would have its own privacy laws (for firms operating in more than one state). I say that because trust accounting Rules in some states are very different in some aspects than ours. And some firms operate in Beijing. Or as a verins.

You might consider adding something about that.

But all in all, I really like the opinions being issued by COPRAC. They are so helpful and my audiences of lawyers, especially in small towns, love the guidance.

--

Carol M. Langford  
Clangford.com  
University of San Francisco School of Law  
2130 Fulton Street  
San Francisco, California 94117-1080

Office:  
1001 Madison Street Fl. 1  
Benicia, California 94510  
707.745.3766

March 12, 2020

Angela Marlaud  
Office of Professional Competence, Planning and Development  
State Bar of California  
180 Howard Street  
San Francisco, CA 94105

Re: Proposed Formal Opinion Interim No. 16-0002 (Data Breaches)

Dear Ms. Marlaud:

On behalf of the California Lawyers Association Ethics Committee and in response to the State Bar of California's request for public comment, we respectfully submit this letter addressing Proposed Opinion 16-0002. The Committee appreciates the opportunity to comment on Proposed Formal Opinion No. 16-0002.

As this opinion notes, it takes the same "on-going engagement" approach to technology as in Cal. State Bar Formal Opinions 2015-193 and 2010-179, albeit with a new technological issue, data breaches, an issue extensively covered in ABA SCEPR Formal Opinion 483. We concur with the analysis in the opinion and applaud COPRAC's efforts on this, and share several comments below.

1. The Digest states that the question is for lawyers to "assess the risks of keeping such data on electronic devices and computers . . ." But it can be assumed that lawyers have no practical choice but to receive, transmit, or keep some confidential client data on electronic devices or computers. The question then is whether to use a specific device, whether to store data on a device or only access data stored elsewhere, and how to protect the information stored on or accessed from a device and in its storage on servers or the cloud.
2. The word "concludes" on the first line of the first paragraph on page 2 should be changed to "concluded" because it is used to refer to prior opinions.
3. The opinion should mention that California Rules of Professional Conduct rule 1.1 does not include an analogue to Comment [8] of the ABA Model Rules regarding keeping abreast of changes in the benefits and risks associated with relevant technology. The draft opinion (in the first paragraph in the Discussion section entitled "Confidentiality and Competency") cites to COPRAC Formal Opinion 2015-193 for the proposition that a lawyer must "have a basic

understanding of the 'benefits and risks associated with relevant technology.'" Because that opinion cited to Comment [8] of ABA Model Rule 1.1, it could be misleading to not mention that California does not currently include this comment.

4. Footnote 3 cites to ABA Formal Opinion 483. Since ABA opinions, other than the most recent ones, are generally unavailable for free to non-ABA members, including a parenthetical or footnote providing some context for each citation could help some readers.
5. The reference in the Discussion section to "law firms should consider preparing a data breach response plan" should be re-considered. If this is merely practice guidance for law firms, rather than an ethical requirement, that should be made clear. Or, in the alternative, the suggestion could be omitted from the opinion.
6. The discussion of Attorney B in "The Factual Scenarios" could be fleshed out more fully to address what Attorney B's choices were, whether Attorney B took reasonable steps to avoid disclosure of client confidential information, and whether Attorney B ran afoul of any lawyer duties. Also, the discussion could include the possibility that Attorney B's cell service provider might have had the ability to lock down the phone, and that Attorney B should have contacted the cell service provider to see what options were available after Attorney B learned that the phone was not within Attorney B's control.
7. The discussion of Attorney D provides that "Attorneys who keep confidential information on their portable devices ought to be aware that accessing public Wi-Fi or other unsecure networks may open another access point for hackers." This can be true of any device, whether or not portable, that use any public or unsecured WiFi network, and the committee should consider adding this point. Also, it is possible a breach may permit access to the entire device, not only the attorney's keystrokes. Information security technology is evolving, and the best practices for protecting data will change over time. The point that we all need to make is that attorneys need to understand the risks, and keep apprised of the technology options available.

Sincerely,



David Majchrzak  
Co-Chair  
California Lawyers Association Ethics  
Committee

Angela Marlaud  
Office of Professional Competence, Planning and Development  
State Bar of California  
180 Howard Street  
San Francisco, CA 94105

Re: COPRAC Proposed Formal Opinion Interim 16-0002 (Data Breaches)

On behalf of the San Diego County Bar Association, we thank you for the opportunity to comment on Proposed Formal Opinion Interim No. 16-0002.

We have reviewed the proposed opinion, and have the following comments.

1. **Need for the opinion.** Some members of our Legal Ethics Committee question the need for a COPRAC opinion on this subject in light of the ABA's comprehensive treatment of the subject in its Formal Opinion 483. However, others on the Committee noted that given the non-binding nature of ABA Ethics Opinions in California, a California opinion on the subject of data breaches is warranted despite the significant overlap between the two opinions.
2. **Citation to authority.** On page 1, the draft opinion cites to Cal. State Bar Formal Opinion No. 2015-193. There, we believe a citation to San Diego County Bar Association Legal Ethics Opinion 2015-1 would also be appropriate. The latter Opinion discusses attorneys' ethical obligations in relation to the storage and transmission of electronically stored information (ESI).
3. **Civil liability.** In the first full paragraph on page 5, the second to last sentence states, in relevant part: "Some security precautions are so readily available and user-friendly ... that failure to implement them could be deemed unreasonable." Some on our Committee were concerned that this language comes perilously close to suggesting a standard for the imposition of civil liability, which is not an appropriate issue for a legal ethics opinion to weigh in on.
4. **Former Clients.** In footnote 3 on page 5, the draft opinion notes that does not address any duty of disclosure to former clients. We believe that the opinion should address that topic, as does ABA Formal Opinion 18-483. The analysis regarding former clients is not terribly complicated, and would not unduly lengthen the current draft opinion. However, virtually every data breach will involve both current and former clients, and many attorneys looking to the opinion will seek guidance with regard to the latter as well as the former.
5. **Conflicts of Interest.** In relation to the discussion of Attorney D on page 8 of the draft opinion, we note that the attorney's handling of the client's confidential information was such that the Attorney might face civil liability to the client. In such circumstances, a conflict of interest might arise between the attorney and client. See ABA Formal Opinion 481 (Lawyer's Duty to Inform a Current or Former Client of the Lawyer's Material Error – discussing potential conflict of interest under ABA Model Rule 1.7(a)(2)). We believe the draft opinion should at least note the

potential for a conflict of interest between Attorney D and the client in the factual scenario presented in the draft opinion.

Thank you for the opportunity to provide input on this opinion.

Sincerely,

San Diego 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

March 27, 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](mailto: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 over 9,000 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 leanings, 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.

First, based on the overall goal of the opinion being to extend the analysis of Formal Opinion No. 2010-179 due to evolving technology, we believe the opinion could be strengthened through use of additional examples that are cutting edge. For example, both Attorney A and Attorney B in the Formal Opinion have similar issues (*i.e.*, the loss of technology (laptop and smartphone) possessing confidential client information). However, there are no examples regarding electronic sharing of confidential information (*e.g.*, drop box or similar links), use of cloud-based document storage, or use of electronic means to upload, store, and present trial exhibits, client documents, or deposition transcripts (*e.g.*, Trial Pad, Transcript Pad, Doc Review Pad), all of which are in increasingly common use. We believe adding such examples could increase the duration in which this opinion is relevant and further the goal of the opinion.

At Page 5, in the second full paragraph, we believe Rule 5.2 should be addressed. For example, a subordinate lawyer should not blindly follow technological rules that are antiquated or fail to act in accordance with the State Bar Act when no rules are established by the law firm but should be.

At Page 8, we believe further discussion regarding Attorney D could strengthen the opinion. We believe the opinion should analyze and conclude whether Attorney D's behavior gives rise to a violation under the principles set forth in Formal Opinion 2010-179. We further believe COPRAC should consider

including a discussion about whether the use of a public network in and of itself is a violation under the principles set forth in Formal Opinion 2010-179. If not a per se violation, what are reasonable steps a lawyer should take before using a public network? We suggest that this could be clarified. Without addressing these issues, the analysis of Attorney D's conduct seems incomplete and in need of a more fulsome analysis.

Throughout the Opinion are references to "confidential client information." COPRAC should explain the differences between confidential client information and attorney-client privileged communications, including that the duty of confidentiality is broader than the attorney-client privilege. Although COPRAC has made this point in several recent opinions, it might be worth a reminder in this context, as so many lawyers do not fully understand the scope of information the duty of confidentiality requires them to protect.

The Opinion refers to the "duty of competency." We suggest the Opinion uses "duty of competence" instead, as that is what is used in Rule 1.1.

In the first paragraph on page 5, the Opinion states, "if a firm allows its staff to work on client matters remotely. . . ." Given that, with few or no exceptions, all lawyers work on client matters remotely, perhaps COPRAC should consider not starting this point with an "if".

In Footnote 3, the Opinion states that it is not addressing the duty of disclosure to former clients. But why not? If a law firm has a data breach, there are likely to be as many, if not more, former clients affected than current clients. The Opinion should provide guidance to lawyers on how to handle such a breach vis-à-vis a former client.

In Footnote 5, the Opinion refers to insurance carriers. Data breaches typically would be covered by a cyber policy, and not by the usual LPL or CGL policy. COPRAC should consider clarifying that point in the footnote.

Although COPRAC rightfully does not opine on liability issues or statutory notification duties, it may be worth a footnote on those points. For example, Attorney D certainly could face a civil lawsuit if client Company suffers damages as a result of Attorney D's conduct. COPRAC may want to note that it is not opining on Attorney D's potential civil liability in this situation.

Thank you for your consideration of our comments and suggestions.

Sincerely,



Scott B. Garner  
2020 President  
Orange County Bar Association



**Los Angeles County Bar Association**

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

Telephone: 213.627.2727 | [www.lacba.org](http://www.lacba.org)

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

Dear Angela:

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

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

- 1) 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 ...."
- 2) Later in the same sentence, "and" should be "or"
- 3) In the top line on page 2, the word "concludes" should be "concluded."
- 4) The concluding sentence of that paragraph, although written in the passive voice, likely will be read to mean that each lawyer has an obligation to be current with technology. In addition to this sentence not being limited to technology used in the practice of law, we think it is important that this be modified to make clear that an individual lawyer should not be subject to criticism for unauthorized electronic access that occurs after technology issues have been delegated to others within a law firm or have been delegated to I.T. consultants outside the law firm, so long as the delegation was reasonable and there has been compliance with rules 5.1 and 5.3. Lawyers are trained only in the law and are licensed after successfully completing an examination of their legal knowledge. While the draft opinion does have some references to I.T. consultants, such as in the first paragraph of the Discussion section, we believe the opinion should not include language that could be quoted out of context to mean that lawyers have a duty that extends to themselves becoming technology

experts. This distinction between the reasonable delegation of I.T. responsibility and personal obligation can be seen from the cited prior COPRAC opinions, but one cannot assume that readers will be so diligent and scholarly as to look at this opinion's cited authorities.

5) The second full paragraph on p. 5 of the draft opinion discusses rule 5.1 and 5.3 obligations. We understand that paragraph to the extent that it involves firm-wide systems, such as VPN installation on all firm laptops, but we are not certain what the opinion intends in suggesting that firm management should have policies and procedures in place for the conduct of firm lawyers and non-lawyer personnel. It would be helpful to readers if some examples were included.

6) In the last complete paragraph on p. 5, we would replace "minimize" with "reduce." The word "minimize" suggests a standard of perfection. The Rules of Professional Conduct are rules of reason, and no lawyer should be criticized for taking reasonable steps to protect confidential client information that turn out to be ineffective. The word "minimize" also is used in the Digest, and we would change that to "reduce."

7) In the last line on p. 5, we recommend removing "clearly." The cited rule and statute state a principle but contain no definition of what is significant. That always is a fact and context-specific issue. See rule 1.4, Cmt. [1].

8) The incomplete paragraph at the top of p. 6 identifies two categories of significant developments within the meaning of rule 1.4 and section 6068(m). The first is the misappropriation, destruction, "or compromising" of confidential client information. The meaning of "compromising" is not certain. If it is intended that this means permitting "unauthorized access" (as we think it should and as opposed to, say, corruption), this should be said directly. The second category is a "cyber breach," and we have two comments about this. First, we do not believe that "breach" adds anything to "unauthorized access" but instead is a narrower category. See paragraph 8, below. Second, we believe that limiting the opinion's application to situations that interfere with a lawyer's ability to represent the client is too narrow a statement of "significant development." A lawyer might think there has been no loss of ability to represent the client if client information is copied but not destroyed, but we believe the unauthorized access nevertheless would be significant. See paragraph 9, below.

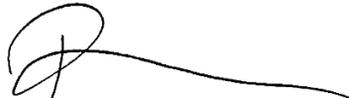
9) We do not understand the purpose of the first complete paragraph on p. 6. It shifts the subject from the question of what is a "significant development" within the meaning of rule 1.4 and section 6068(m) to the question of the definition of "data breach." We don't understand what role that definition has in the draft opinion. We agree that qualified persons should investigate to learn the scope and details of any possible unauthorized access into a law firm's electronic information, but that obligation has nothing to do with whether the event was a "data breach." The draft opinion's statement of the Issue being addressed is phrased in terms of "unauthorized access," and we agree with that language and focus. Note that, as stated in the first paragraph of the Introduction, the problem is broader than an attack on a lawyer's computer system – the apparent meaning of a breach – and includes the loss of electronic devices.

10) We do not agree with the ABA opinion standard used in the second complete paragraph on p. 6 but do agree with the final sentence of that paragraph. The support for that final sentence is not the risk that the client will be adversely affected by unauthorized electronic access but the lawyer's obligation to maintain the client's "confidence" in the lawyer under Bus. & Prof. Code section 6068(e)(1). See *Anderson v. Eaton*, 211 Cal. 113, 116 (1930), which highlights the difference between "confidence" [there is no "s"] and "secrets" in what now is section 6068(e)(1): "One of the principal obligations which bind an attorney is that of fidelity, the maintaining inviolate the confidence reposed in him by those who employ him, and at every peril to himself to preserve the secrets of his client." This is repeated in *Responsible Citizens v. Superior Court*, 16 Cal. App.4th 1717, 1728 (1993). A lawyer's obligation of fidelity to the client includes the requirement that the lawyer place the client's interest above the lawyer's own interests, including the lawyer's desire to avoid personal embarrassment. See also, *Neel v. Magana, Olney, Levy, Cathcart & Gelfand*, 6 Cal.3d 176, 188-89 (1971). The Digest also speaks of negative impact on the client, and that should be coordinated with the body of the opinion. Any development is significant if a reasonable client would want to be told about it and if the failure to disclose foreseeably would interfere with the client's willingness to trust the lawyer.

11) There is a typo in the paragraph immediately preceding the section titled The Factual Scenarios. "HIPPA" should be "HIPAA"

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

Sincerely,

A handwritten signature in black ink, appearing to read 'Brandon Niles Krueger', with a long horizontal flourish extending to the right.

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