

CLEAN

DRAFT # 13, Submitted for December 6, 2019, meeting

*Roche
Bundy
Fields
Krueger

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

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: California Rules of Professional Conduct: 1.1, 1.4, 1.6, 5.1, 5.2 and 5.3
California Business & Professions Code § 6068(e), (m);
California Civil Code § 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

CLEAN

confidentiality. 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 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 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 texts 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 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

CLEAN

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, and 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 (CRPC, Rule 1.1) and the duty to safeguard clients' confidences and secrets (Rule 1.6 and B&P Code sec. 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.¹

ABA Formal Opn. 483 (2018) on 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 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 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 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 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 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 updated in response to new developments.” *Id.* (quoting from the ABA Cybersecurity Handbook at 73).

¹ Discussed in ABA 483 at pp. 6-7 and in the ABA Cybersecurity Handbook.

“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 CRPC 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 offices resources connected to the internet and external data sources. ABA 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 principle 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

CRPC 1.4(a)(3) and B&P § 6068(m) require attorneys to keep their clients² “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 “significant.” (See, e.g., Tuft & Peck, The Rutter Group Guide to Professional Responsibility, § 6:128, acknowledging that what is “significant” under these provisions varies with each client’s needs and the nature of the

² This opinion focuses on current clients and does not address the duty of disclosure owed to former clients. See discussion of this in ABA 483 at 13-14.

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 483 at 10; N.Y. State Bar Committee on Professional Ethics Opn. 842 (2010) (involving a data breach of a cloud storage provider); ABA Formal Opn. 95-398 (1995).

ABA Formal Opinion 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 483 at p. 4³. 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. (ABA at 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 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.⁴ For example, affected

³ 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.

⁴ Lawyers and law firms should also consider notifying malpractice carriers as soon as possible of any circumstances giving rise to a potential breach to put the carrier on notice. The carrier will likely also be able to help determine if there are any immediate steps that can be taken to mitigate potential harm to clients and help evaluate whether notice to affected clients is necessary or recommended. Policies typically have fairly short time limits within which notice must be given. The carrier may also guide attorney in crafting a disclosure to affected clients that both satisfies attorney’s ethical duties and is consistent with the obligations of Attorney’s insurance policy.

clients might want or need to change passwords and modify or delete on-line accounts. 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 483 at p. 14.

Lawyers may also have notification obligations under Cal. Civil Code sec. 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

CLEAN

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. COPRAC Formal Opn. 2010-179 at 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 483 at 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

CLEAN

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 the result of technology use, to monitoring 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.