

1 DRAFT # 11, Submitted for September 6, 2019, meeting

2
3
4
5
6
7

8 **THE STATE BAR OF CALIFORNIA**
9 **STANDING COMMITTEE ON**
10 **PROFESSIONAL RESPONSIBILITY AND CONDUCT**
11 **DRAFT FORMAL OPINION INTERIM NO. 16-0002**
12 **THE ETHICS OF RESPONDING TO CYBER RISKS**

13 **ISSUES:** What are a lawyer's ethical obligations when electronically stored client
14 confidential information is acquired by third persons without
15 authorization?

16 **DIGEST:** Attorneys who carry portable electronic devices which contain
17 confidential information must assess the risks of keeping electronic data
18 on portable devices and take reasonable steps to secure their electronic
19 systems to minimize the risk of unauthorized access. In the event of a
20 breach, they may have to notify affected clients if confidential information
21 stored on them is accessed or potentially accessed. Discipline may also
22 be imposed if a pattern of incompetent practices or recklessness is shown.

23 **AUTHORITIES**

24 **INTERPRETED:** California Rules of Professional Conduct: 1.1; 1.4; 1.6
25
26 California Business & Professions Code § 6068(e), (m);
27 California Civil Code § 1798.82

28

29 **STATEMENT OF FACTS**

30 **Attorney A (he/him/his)**

31

32 Attorney A's laptop is stolen while going through TSA screening at an airport. The laptop
33 contained confidential client information that was unencrypted and did not have software
34 installed that allowed it to be remotely erased or locked down. It required a 4-character password
35 before giving access to any of the programs, but once the password is entered, all programs and
36 applications on the computer are available.

37

CLEAN

Attorney B (she/her/hers)

At the end of a busy day, Attorney B meets a colleague for dinner at a restaurant. Waiting for her colleague to arrive, she checks her business and personal e-mail on her smartphone. B does not use a password, PIN, or biometric security feature.

In the process of getting ready to go to bed, Attorney B suddenly realizes that she left her cell phone in the restaurant. She immediately calls the restaurant, but it is closed. B goes to the restaurant when it opens the next morning. The restaurant manager assures her that an employee saw the phone on the table, brought it to the manager, and that it was placed in a lost and found drawer from which he retrieves it.

Law Firm C

Law Firm C is a four-member firm, specializing in corporate law. The 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 the 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 the firm's server. She did so, and malicious software (ransomware) installed itself on the firm's network, immediately locked up the firm's computers, and displayed a message demanding that a sum of money be transferred electronically by bitcoin to unlock the firm's computers. In consultation with security experts, the Law Firm determined that no client information was accessed and none of the matters being handled by the firm were negatively impacted by the delay. The firm paid the ransom and regained access to its data.

Attorney D (they/them/their)

Attorney D is in-house counsel for a publicly traded pharmaceutical company that has been working on a cure for Alzheimer's disease. On vacation, Attorney goes to a coffee shop and accesses the shop's public Wi-Fi network to check their e-mail and conduct some personal business. 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 they actually logged on to that fake network. Attorney's laptop was not encrypted. Unbeknownst to Attorney D, the hacker sitting in the coffee shop with keystroke tracking software could see the text that people logged on to the fake network were typing on their laptops. The hacker read an e-mail that Attorney D wrote to the Company's marketing team which discussed a breakthrough on the Alzheimer's drug that was about to be publicly announced. The hacker immediately purchased stock in the company and made a large profit when the news was announced. The S.E.C. interviews company officials about the anomalous trade and the source of the information is revealed internally.

DISCUSSION

Background

Every year, more than 625,000 laptops are lost in U.S. airports alone.¹ In 2014, over 5 million cell phones were lost or stolen in the U.S., and countless Americans misplace briefcases every day.² When these items belong to an attorney and involve the loss of client information, in addition to the inconvenience involved, there are ethical concerns, which may require an attorney to take certain remedial steps. Similarly, law firms are becoming more enticing targets for data thieves because the client information held by the firm is valuable. “According to the American Bar Association, 22 percent of more than 4,000 respondents in the 2017 ABA Legal Technology Survey said their firms had experienced a data breach in 2017, up from 14 percent in 2016. Of all survey respondents, 25 percent reported having no policies, with small firms leading in that category, and 7 percent of all respondents said they did not know about security policies.”³ A recent title of an on-line news report puts it starkly: “Hackers are aggressively targeting law firms’ data.”⁴

Introduction

In COPRAC Formal Opn. 2015-193, we discussed attorneys’ ethical obligations when dealing with e-discovery, and in COPRAC Formal Opn. 2010-179 we 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, we adopted an approach that posed questions lawyers should consider in order to comply with the duties of competency and confidentiality. In light of the changing technology, we concluded 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 attendant on the use of electronic devices that contain client confidential information and connect to the internet and thus are theoretically accessible to anyone with an internet connection. We start with a useful description of data breaches: “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 Formal Opn. 483 at p. 4 (2018) (hereafter ABA 483).

Confidentiality and Competency

The duty of competency (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 that information. The threshold requirement is for lawyers to have a basic understanding of the

¹ http://www.dell.com/downloads/global/services/dell_lost_laptop_study.pdf

² <http://www.consumerreports.org/cro/news/2015/06/smartphone-thefts-on-the-decline/index.htm>

³ <https://www.natlawreview.com/article/law-firms-and-cyber-attacks-what-s-law-firm-to-do-part-one>

⁴ <https://www.cio.com/article/3212829/cyber-attacks-espionage/hackers-are-aggressively-targeting-law-firms-data.html>

“benefits and risks associated with relevant technology.” COPRAC Formal Opn. 2015-193. This general principle requires lawyers to have a basic understanding of the risks posed 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 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 app 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 network and if the data is not adequately protected. And the threats vary and widen as data thieves develop their attack strategies and as technologies develop.⁵ Thus, lawyers must understand how their particular use of electronic devices and systems post risks of unauthorized access, they must be knowledgeable about the options available at any given point in time to minimize those risks, and they then must implement reasonable security measures in light of the risks posed. In addition, because law firms are frequent targets, firms ought to consider preparing a data breach response plan so that all stakeholders know how to respond when a breach occurs.⁶

ABA 483 provides a useful list of competence-based duties that flesh out the requirement of “reasonable efforts” in handling confidential information in electronic form:

- 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 do not create a strict liability standard. Nor does the duty “require the lawyer to be invulnerable or

⁵ For example, there may be significant security concerns with installing a “smart speaker,” such as Amazon’s Alexa for Business, in a law office. <https://www.questia.com/library/journal/1G1-542404783/smart-speakers-raise-privacy-and-security-concerns>.

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

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).

“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 would be deemed unreasonable. Others will require a deeper assessment.

Finally, in law firms with subordinate lawyers, partners, particularly those with management responsibilities, should be aware of RPC rules 5.1 and 5.3. Rule 5.1 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.” And Rule 5.3 makes this 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 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 subordinate lawyers and staff to be kept up to date on the firm’s evolving protective measures as they are implemented.

Duty of Disclosure

CRPC 1.4(a)(3) and B&P § 6068(m) require attorneys to keep their clients⁷ reasonably apprised of any “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.*, Mark Tuft & Elaine 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 representation.) Nevertheless, the authorities which have opined on the issue of whether the misappropriation, destruction, or compromising of client confidential information, or whether a cyber breach has significantly impaired the lawyer’s ability to provide legal services to clients is a “significant development” have concluded in the affirmative. *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).

⁷ 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.

Lawyers and clients may well differ as to what events would trigger the duty to disclose. The key principle, in the data breach context, is if the breach harmed a client or clients or is reasonably foreseeable to have harmed or cause future harm to clients. Notification is essential because the client will likely have to make decisions relevant to the breach (such as the need to take mitigating measures) and/or how the client's matter will be handled going forward. When in doubt, lawyers should assume that their clients would want to know of a breach and be appropriately notified.

The Factual Scenarios:

Attorney A's handling of the electronic data on his laptop posed a high risk of harm to the firm's clients. The hypothetical facts contain several problematic details, such as keeping client information on portable electronic devices in unencrypted format, with no or easily hackable passwords, and without the ability to remotely locate or erase the data post-theft. The apparent failure of the firm to give serious thought to the cyber risks attendant on keeping confidential information in unencrypted form on its members' laptops and to supervise its members' use of laptops is problematic, at least on the part of managing partners. Although Attorney A does not know that an unauthorized person accessed the data, it must be assumed that the stored data has been compromised. The duty to disclose would also apply where there is a substantial likelihood that confidential information was been misappropriated, destroyed, or compromised. Thus, here, Attorney A will likely have to inform his clients that his laptop containing their confidential information has been stolen. The extent or detail required in such a disclosure is discussed below.

On the other hand, Attorney B's temporary loss of her smartphone, under the circumstances, might not pose the same risk, particularly if she can obtain assurances from the restaurant owner/staff that only they had access to it and that none of them accessed the phone's contents while it was there. Because it does not appear that the data on Attorney B's phone was misappropriated, destroyed or compromised, the temporary loss of the phone would not constitute a significant development and no duty to disclose would be triggered.

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."⁸ Given the ubiquity of this method of gaining access, solo practitioners and firms must consider and implement reasonable precautions, such as staff and attorney training, protocols for handling in-coming e-mails, and the like. 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 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.

⁸ The cyber risk is apparently heightened if the firm is using older operating systems, such as Windows XP, which are no longer receiving security updates or if security patches and updates are not installed in newer versions. A Chicago law firm has been sued by a former client because of a data breach allegedly facilitated by the firm's failure to update its server software.

<https://www.casemine.com/judgement/us/5914d86cadd7b0493487a75f>

CLEAN

Attorneys who keep confidential information on their portable devices ought to be aware that accessing public Wi-Fi 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 (that is, on portable devices) 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 allowing a hacker to misappropriate and profit from that information. Regardless of whether the insider trading financially harmed the client, 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. Of course, the event would also require Attorney D to take appropriate remedial steps in terms of future on-line activities in unsecured locations.

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

In all cases of unauthorized access, disclosure to clients must be made immediately so the affected clients can take steps to ameliorate the harm. For example, affected clients might want or need to change passwords and modify or delete on-line accounts.⁹ Given the importance of preserving 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, "it must provide enough information for the client to make an informed decision as to what to do next, if anything. In a data breach scenario, the minimum disclosure required to all affected clients under Rule 1.4 is that there has been unauthorized access to or disclosure of their information, or that unauthorized access or disclosure is reasonably suspected of having occurred. Lawyers must advise clients of the known or reasonably ascertainable extent to which client information was accessed or disclosed. If the lawyer has made reasonable efforts to ascertain the extent of information affected by the breach but cannot do so, the client must be advised of that fact." 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.¹⁰

CONCLUSION

⁹ Attorney A should also consider notifying his malpractice carriers of the circumstances to allow the carrier to take critical initial steps to mitigate possible harm, to determine whether notice to affected clients will be necessary, and to avoid the risk of absolving the carrier to provide a defense and indemnification should a claim be made. Policies typically have fairly short time limits within which notice must be given.

¹⁰ See https://oag.ca.gov/system/files/LT%20Clients%20Sample%20w%20How%20To_1.pdf for a notification letter from a California law firm flowing from a ransomware attack; HIPPA notification regulations: 45 CFR secs. 164.400-414; EU GDPR official site: <https://eugdpr.org/>

CLEAN

271 The use of computers and portable electronic devices by lawyers is now ubiquitous and has
272 increased the risk of client confidential information falling into or being snatched by
273 unauthorized hands. Lawyers have an affirmative, non-delegable duty to assess the risks
274 involved in the use of electronic devices holding confidential information and to take reasonable
275 precautions to ensure that that information remains secure. Creation of a data breach plan could
276 be a useful tool to identify the risks posed to the firm's then-current use of technology and
277 feasible precautions. The assessment of risk might also include consulting with appropriate
278 technology experts.

279