

CLEAN

DRAFT #9, Submitted for , April 18, 2019, meeting

\*Solomon  
Deitz  
Roche  
Bundy  
Bomse

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

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

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

**AUTHORITIES**

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

**STATEMENT OF FACTS**

**Attorney A**

Attorney A's laptop is stolen while goes through TSA screening at an airport.

The laptop contained confidential client information that was unencrypted and did not have software installed that allowed it to be remotely erased or locked down. It required a 4-character password before giving access to any of the programs, but once the password is entered, all programs and applications on the computer are available.

**Attorney B**

At the end of a busy day, Attorney B realized she has lost her briefcase. Attorney B used her briefcase to transport hard copies of client files, or documents she is currently working on, back and forth between her home and her law office. For convenience, she also stores her cell phone in the pocket of the briefcase designed for such use.

Attorney B keeps no inventory of what is in the briefcase at any one time and is continually putting things in and taking things out according to her needs. Although she does not know exactly what was in the briefcase when it was lost, she does know that it contained confidential information and her cell phone, as she cannot find it.

In the process of getting ready to go to bed, Attorney B suddenly realizes that she left her briefcase in the restaurant where she had had dinner with a colleague and a client. She immediately calls the restaurant, but it is closed. B goes to the restaurant when it opens the next morning and retrieves her briefcase. Nothing appears to be missing.

**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, unknowingly and unwittingly unleashing ransomware which 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 transom and regained access to its data.

**Attorney**

Attorney 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 his e-mail and conduct some personal business. He doesn't realize that he actually logged on to a fake network set up by a hacker that resembled the legitimate one. Attorney's laptop was not encrypted. Unbeknownst to Attorney, the hacker sitting in the coffee shop gained access to her laptop and, with keystroke tracking software read an e-mail that Attorney E 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.<sup>1</sup> In 2014, over 5 million cell phones were lost or stolen in the U.S., and countless Americans misplace briefcases every day.<sup>2</sup> 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 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.”<sup>3</sup> A recent title of an on-line news report puts it starkly: “Hackers are aggressively targeting law firms’ data.”<sup>4</sup>

**Introduction**

In COPRAC Formal Opn. 2015-193, we discussed attorney’s 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 to comply with the duty of competency. In light of the changing technology, we concluded that an on-going engagement with that evolving technology in the form of 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 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 “benefits and risks associated with relevant technology.” COPRAC Formal Opn. 2015-193. This

<sup>1</sup> [http://www.dell.com/downloads/global/services/dell\\_lost\\_laptop\\_study.pdf](http://www.dell.com/downloads/global/services/dell_lost_laptop_study.pdf)

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

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

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

general principle requires lawyers to have a basic understanding of the risks posed by the use of a given technology and, if necessary, obtain help from appropriate technology experts on assessing those risks and taking reasonable steps to prevent data breaches. Thus, encrypting email, use of strong passwords, staff training to detect email attacks, and the like should be considered. Similarly, since larger law firms seem to be more attractive targets than solo practitioners, firms ought to consider preparing a data breach response plan so that all stakeholders know how to respond when a breach occurs. Once a breach has occurred, 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 of confidentiality requires reasonable efforts to prevent inadvertent or unauthorized disclosure or unauthorized access to client confidential information. This flows from the duty to safeguard clients’ confidences and secrets under Rule 1.6 and B&P Code sec. 6068(e).

Rules 1.1 and 1.6 impose a duty to make reasonable efforts to preserve client confidential information, and thus do not create a strict liability standard. Nor do they “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 and is thus relative. 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.

In light of this standard and the ethical duty to be cognizant of the risks posed by storing client confidential information electronically, attorneys would be expected to be aware of, and to implement, readily available technologies to minimize the risk of inadvertent disclosure. For example, the process of analyzing a law or law firm’s electronic data use could lead to, for example, accessing needed information with their laptops through a virtual private network (VPN), which encrypts the data stream in both directions, and not keeping that data on the laptop itself. Practice management programs typically include a secure remote access feature that can be

set up to maintain all client information in cloud storage. Alternatively, all data on laptops and other portable devices can be encrypted and protected with a strong password or two-factor authentication<sup>5</sup> Software can be installed on portable devices that allow the device to be locked and/or the data erased in the case of loss or theft. And attorneys and staff can be trained to spot and appropriately respond to suspicious e-mails.

### **The Factual Scenarios:**

Attorney A’s handling of the electronic data on his laptop would seem to squarely breach the duty of confidentiality if an unauthorized person gained access to protected information. 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.<sup>6</sup> Although Attorney A does not know that an unauthorized person accessed the data, it must be assumed that the stored data has been compromised.

On the other hand, Attorney B’s temporary loss of her briefcase, under the circumstances, might not pose the same risk, particularly if she can obtain assurances from the restaurant owner/staff that no one opened the briefcase and accessed its contents while it was there.

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.”<sup>7</sup> 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.

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’s exposing confidential information to anyone with the capability of electronically “eavesdropping” on the Attorney’s key strokes. Attorneys who work on client matters remotely (that is, on portable devices) must also 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).

---

<sup>5</sup> “Organizations should consistently use strong encryption to protect personal information on laptops and other portable devices. . . .” *California Data Breach Report*, Calif. Dept. of Justice, p. vi (Feb. 2016). Encryption with a strong password renders the laptop a “brick,” i.e., unusable by anyone without the password.

<sup>6</sup> Comment 1 to Rule 1.1 refers readers to rules 5.1 and 5.3 which deal with lawyers’ ethical responsibility to supervise subordinate lawyers and non-lawyers.

<sup>7</sup> 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.

## **Duty of Disclosure**

CRPC 1.4(a)(3) and B&P § 6068(m) require attorneys to keep their clients<sup>8</sup> 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). Lawyers and clients may well differ as to what events would trigger the duty to disclose. The key factor is whether the event requires or creates an opportunity for the client 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 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.

Similarly, because it does not appear that the contents of Attorney B’s briefcase were misappropriated, destroyed or compromised, the temporary loss of the briefcase would not constitute a significant development and no duty to disclose would be triggered.

Law Firm C has certainly been inconvenienced by the cyber breach, but the firm has confirmed that 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. Correspondingly, the firm would not be required to disclose the incident.

Attorney’s failure to secure her on-line communications exposed confidential information allowing a hacker to misappropriate and profit from that information. Although the insider trading did not financially harm the client [*is this correct?*], 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, it would also require Attorney E to take appropriate remedial steps in terms of future on-line activities in unsecured locations.

---

<sup>8</sup> This opinion focuses on current clients and does not address the duty of disclosure owed to former clients. Attorneys are well advised to consider their document retention policies and the advisability of describing the attorney’s document retention protocol in retainer agreements. *See* discussion of this in ABA 483 at 13-14.

## CLEAN

In all cases of unauthorized access, prudence dictates that disclosure to clients 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, modify or delete on-line accounts, and the like.<sup>9</sup> 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 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.<sup>10</sup>

## CONCLUSION

The use of computers and portable electronic devices by lawyers is now ubiquitous and has increased the risk of client confidential information falling into or being snatched by unauthorized hands. Lawyers have an affirmative, non-delegable duty to assess the risks involved in the use of electronic devices holding confidential information and to take reasonable precautions to ensure that that information remains secure. The assessment of risk might also include consulting with appropriate technology experts. Fortunately, many, if not most, of those steps are readily available and relatively easy to acquire and use. If the unauthorized person uses them to harm the lawyer’s clients, the failure to have taken reasonable precautions is likely to harm the lawyer both professionally and financially.

---

<sup>9</sup> 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.

<sup>10</sup> See [https://oag.ca.gov/system/files/LT%20Clients%20Sample%20w%20How%20To\\_1.pdf](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/>