

DRAFT #, 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.

CLEAN

37 Attorney B

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

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

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

50 Law Firm C

51 Law Firm C is a four-member firm, specializing in corporate law. The firm's receptionist
52 routinely receives e-mails sent to the firm (rather than to a specific attorney or staff member),
53 and routes them to the appropriate person. Just before quitting time, the receptionist received an
54 e-mail from a business purporting to be the firm's IT provider; it looked entirely genuine and
55 asked the receptionist to click on the attachment to allow the firm to do routine maintenance on
56 the firm's server. She did so, unknowingly and unwittingly unleashing ransomware which
57 immediately locked up the firm's computers and displayed a message demanding that a sum of
58 money be transferred electronically by bitcoin to unlock the firm's computers. In consultation
59 with security experts, the Law Firm determined that no client information was accessed and none
60 of the matters being handled by the firm were negatively impacted by the delay. The firm paid
61 the transom and regained access to its data.

62 Attorney

63 Attorney is in-house counsel for a publicly traded pharmaceutical company that has been
64 working on a cure for Alzheimer's disease. On vacation, Attorney goes to a coffee shop and
65 accesses the shop's public Wi-Fi network to check his e-mail and conduct some personal
66 business. He doesn't realize that he actually logged on to a fake network set up by a hacker that
67 resembled the legitimate one. Attorney's laptop was not encrypted. Unbeknownst to Attorney,
68 the hacker sitting in the coffee shop gained access to her laptop and, with keystroke tracking
69 software read an e-mail that Attorney E wrote to the Company's marketing team which
70 discussed a breakthrough on the Alzheimer's drug that was about to be publicly announced. The
71 hacker immediately purchased stock in the company and made a large profit when the news was
72 announced. The S.E.C. interviews company officials about the anomalous trade and the source of
73 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 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

Confidentiality and Competency

In COPRAC Formal Opn. 2015-193, we discussed attorney’s ethical obligations when dealing with e-discovery. We opined that “the duty of competency requires an attorney to assess at the outset of each case what electronic discovery issues might arise during the litigation, including the likelihood that e-discovery will or should be sought by either side. If e-discovery will probably be sought, the duty of competence requires an attorney to assess his or her own e-discovery skills and resources as part of the attorney’s duty to provide the client with competent representation. If an attorney lacks such skills and/or resources, the attorney must try to acquire sufficient learning and skill, or associate or consult with someone with expertise to assist.”

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.

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. In assessing whether a lawyer has made reasonable efforts to prevent unauthorized access or disclosure, Comment 18 to ABA Model Rule 1.6 lists six, non-exclusive factors:

“the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect 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>

CLEAN

106 lawyer's ability to represent clients (e.g., by making a device or important piece of
107 software excessively difficult to use)."

108 The factor approach is appropriate because it captures the need for lawyers to continually
109 analyze the cyber risks inherent in the use of their electronic data systems and the changing
110 nature of technology. Hard and fast, "brightline" requirements provide a false sense of security
111 and would therefore be counter-productive.

112 We have opined that "attorneys should take reasonable steps as a precautionary measure to
113 protect against disclosure. For example, depositing confidential client mail in a secure postal box
114 or handing it directly to the postal carrier or courier is a reasonable step for an attorney to take to
115 protect the confidentiality of such as mail, as opposed to leaving the mail unattended in an open
116 basket outside of the office door for pick up by the postal service. Similarly, encrypting email
117 may be a reasonable step for an attorney to take in an effort to ensure the confidentiality of such
118 communications remain so when the circumstances call for it, particularly if the information at
119 issue is highly sensitive and the use of encryption is not onerous. . . . Likewise, activating
120 password protection features on mobile devices, such as laptops and [mobile phones], presently
121 helps protect against access to confidential client information by a third party if the device is lost,
122 stolen or left unattended." COPRAC Formal Opn. 2010-179.⁵ In light of the heightened cyber
123 risks now unfortunately embedded in the practice of law, attorneys *must* take reasonable
124 precautionary measures to minimize, if not prevent, unauthorized disclosures.

125 This duty is clearly required by CRPC 1.1, which provides, "a member shall not intentionally,
126 recklessly, with gross negligence, or repeatedly fail to perform legal services with competence."
127 The rule describes competency as the duty to "apply the (i) learning and skill, and (ii) mental,
128 emotional, and physical ability reasonably necessary for the performance of such service." This
129 incorporates the obligation to have and "maintain learning and skill consistent with an attorney's
130 duty of competence [which] includes keeping 'abreast of changes in the law and its practice,
131 including the benefits and risks associated with relevant technology, . . .'" State Bar of California
132 Formal Opinion 2015-193.

133 Thus, competency applies not only to lawyers' knowledge about their areas of practice but also
134 to ancillary matters "reasonably necessary" to enable client representation. If, therefore, lawyers
135 use electronic devices, the duty of competency would require them to be sufficiently aware of
136 the risks associated with storing sensitive information electronically or physically, and, in the
137 case of the former, to take precautions (e.g. passwords, encryption, virtual private networks, file
138 back-ups, and the like) consistent with this awareness. COPRAC Formal Opn. 2012-184 ("This
139 Committee has recognized that while Attorney is not required to become a technology expert in
140 order to comply with her duty of confidentiality and competence, Attorney does owe her clients a
141 duty to have a basic understanding of the protections afforded by the technology she uses in her
142 practice. If Attorney lacks the necessary competence to assess the security of the technology, she

⁵ "Even apart from . . . the use of technology, attorneys have a duty to take reasonable precautions to protect their client's confidential information. . . For example, an attorney who keeps files both in paper form and on an internet server may employ the most up-to-date security precautions for his server, but then fail to lock the door to his office, thereby allowing anyone to come in and rifle through his clients' papers." California State Bar Formal Opinion No. 2012-184, fn 8.

CLEAN

must seek additional information, or consult with someone who possesses the necessary knowledge, such as an information technology consultant.”). See also, State Bar of California Formal Opinion 2010-179; ABA Model Rule of Professional Conduct 1.1, Comment 8 (“To maintain the requisite knowledge and skill, a lawyer should keep abreast of . . . the benefits and risks associated with relevant technology.”); Arizona Ethics Opn. 09-04 (lawyers should “recognize their own competence limitations regarding computer security. . .”).

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 Formal Opinion 483 at p. 9 (2018) [hereafter ABA 483]. 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 authentication⁶ 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.

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

⁶ “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.

problematic, at least on the part of managing partners.⁷ 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."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.

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.

[the consensus seemed to favor deleting this paragraph; I disagree because lawyers ought to be warned that gross negligence could lead to discipline and the facts suggest that some of our hypothetical lawyers could indeed have deemed grossly negligent]

Duty of Disclosure

CRPC 1.4(a)(3) and B&P § 6068(m) require attorneys to keep their clients⁹ 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

⁷ 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.

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.

⁹ 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 pp. 13-14.

CLEAN

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, p. 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 p. 14. Of course, it would also require Attorney E to take appropriate remedial steps in terms of future on-line activities in unsecured locations.

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.¹⁰ Given

¹⁰ 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.

CLEAN

236 the importance of preserving client confidences, secrets and propriety information, it is
237 appropriate to assume that reasonable clients would want to be notified if any of that information
238 was acquired by unauthorized persons.

239 With respect to the details of a required disclosure, “it must provide enough information for the
240 client to make an informed decision as to what to do next, if anything. In a data breach scenario,
241 the minimum disclosure required to all affected clients under Rule 1.4 is that there has been
242 unauthorized access to or disclosure of their information, or that unauthorized access or
243 disclosure is reasonably suspected of having occurred. Lawyers must advise clients of the known
244 or reasonably ascertainable extent to which client information was accessed or disclosed. If the
245 lawyer has made reasonable efforts to ascertain the extent of information affected by the breach
246 but cannot do so, the client must be advised of that fact.” ABA 483 at p. 14. Lawyers may also
247 have notification obligations under Cal. Civil Code sec. 1798.82 and federal and international
248 laws and regulations such as HIPPA and the EU General Data Protection Regulation.¹¹

CONCLUSION

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

¹¹ 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/>