

CLEAN

DRAFT #8, Submitted for January 11, 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
LOST OR STOLEN LAPTOPS AND BRIEFCASES**

ISSUES: What are a lawyer's ethical obligations when an attorney's laptop, cell phone or briefcase containing client confidential information is either lost or stolen? *[if the Committee likes the additional hypotheticals, this will be revised to incorporate them]*

DIGEST: Attorneys who carry portable electronic devices which contain confidential information may have to notify affected clients if those devices are stolen or lost and cannot be remotely located or have the stored data erased, particularly if the data stored on those devices is unencrypted and not protected with an appropriate password. Similarly, attorneys who carry confidential information in a briefcase that is stolen or lost may also face the same notice obligation. Discipline may also be imposed if a pattern of incompetent practices or recklessness is shown. *[ditto]*

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 goes through TSA screening at an airport. After putting his firm-purchased laptop on the conveyor belt which takes it for X-ray screening, he is told that he has been randomly selected for a manual full body search, which takes a few minutes. After being cleared by the TSA, he goes to the end of the conveyor belt to retrieve his laptop but is not there. A review of

CLEAN

the security tape shows a stranger took his laptop from the conveyor belt while he was being searched. The stranger is nowhere to be found. Attorney A filed a “Lost Property” form with the airport and the TSA, but the laptop has not been recovered and is considered stolen.

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. *[insert details of the contents here]* 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 ransom and regained access to its data.

Law Firm D

Law Firm D is an established personal injury firm. The firm fires a staff member for serious performance problems. The separation was not amicable, and the staff member left quite

CLEAN

embittered. This was the first staff member to be terminated, and the firm did not have a protocol in place for deleting departing employees' passwords and thus their ability to access the firm's computerizing data. Angry, the former employee accesses the firm's computer the day after being terminated and downloads a cache of highly sensitive information pertaining to a particular plaintiff the firm is representing. He then mails the documents to opposing counsel without a return address or other identifying information. The Law Firm partner handling the matter becomes suspicious during his client's deposition because the nature of some of the questions strongly suggest access to confidential information which had not been disclosed during preliminary discovery.

Attorney E

Attorney E 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 what he thinks is the shop's public wifi 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 Attorney's stored e-mails one of which revealed 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. *[help! How does Attorney learn that he's been hacked in this new scenario?]*

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

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>

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

The factor approach is appropriate because it captures the need for lawyers to continually analyze the cyber risks inherent in the use of their electronic data systems and the changing nature of technology. Hard and fast, “brightline” requirements provide a false sense of security.

We have opined that “attorneys should take reasonable steps as a precautionary measure to protect against disclosure. For example, depositing confidential client mail in a secure postal box or handing it directly to the postal carrier or courier is a reasonable step for an attorney to take to protect the confidentiality of such as mail, as opposed to leaving the mail unattended in an open basket outside of the office door for pick up by the postal service. Similarly, encrypting email may be a reasonable step for an attorney to take in an effort to ensure the confidentiality of such communications remain so when the circumstances call for it, particularly if the information at issue is highly sensitive and the use of encryption is not onerous. . . . Likewise, activating password protection features on mobile devices, such as laptops and [mobile phones], presently helps protect against access to confidential client information by a third party if the device is lost, stolen or left unattended.” COPRAC Formal Opn. 2010-179.⁵ In light of the heightened cyber

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.

risks now unfortunately embedded in the practice of law, attorneys *must* take reasonable precautionary measures to minimize, if not prevent, unauthorized disclosures.

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

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

CLEAN

(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 problematic, at least on the part of managing partners.⁷ Although Attorney A does not know that an unauthorized person has accessed the data, it must be assumed that someone at least tried to access it because the device was obtained by theft.

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 concerns motivating this opinion are the misappropriation, destruction, or compromising of confidential information or the significant impairing of the attorney's ability to provide legal services. ABA 483 at p. 4. Here, it does not appear that client confidential information was misappropriated, destroyed, or compromised.

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.

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.

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.

Similarly, Law Firm D failed to terminate the employee's access to its electronic systems and apparently had not developed a protocol for revoking access privileges for attorneys and staff leaving the firm. Terminating a departing employee's access is a widely accepted protective measure, and relatively easy to accomplish. .

Attorneys who keep confidential information on their portable devices ought to be aware that accessing public wifi may open another access point for hackers. This is illustrated by Attorney E'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 inadvertent disclosure of client secrets or privileged information could subject attorneys to professional discipline, particularly if caused by reckless or grossly negligent, preventable behavior. *See, generally*, State Bar of California Formal Opinion 2016-195; *Ainsworth v. State Bar* (1988) 46 Cal. 3d 1218, 1222, 1223 (lawyer disciplined for, among other misdeeds, disclosing clients' confidential information without authorization); *In the Matter of Johnson* (Rev. Dept. 2000) 4 Cal. State Bar Ct. Rptr. 179 (same). And, similarly, the failure to act competently in a manner that is intentional, reckless, or repeated that would result in discipline rule 3-110 violation." State Bar of California Formal Opinion 2015-193. We do not opine on whether the conduct described in either hypothetical would be sufficient for imposing discipline.

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 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

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.

CLEAN

268 handled going forward. When in doubt, lawyers should assume that their clients would want to
269 know of a breach and be appropriately notified.

270 The duty to disclose would also apply where there is a substantial likelihood that confidential
271 information was been misappropriated, destroyed, or compromised. Thus, here, Attorney A will
272 likely have to inform his clients that his laptop containing their confidential information has been
273 stolen. The extent or detail required in such a disclosure is discussed below.

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

277 Law Firm C has certainly been inconvenienced by the cyber breach, but the firm has confirmed
278 that no confidential information was accessed, and the delay did not impair the firm's attorneys
279 from continuing to provide necessary legal services to its clients. Correspondingly, the firm
280 would not be required to disclose the incident.

281 The scenario involving Law Firm D, in contrast, is in flux and it is unclear whether the
282 misappropriation has compromised the client's interests and/or substantially impaired the firm's
283 ability to provide legal services. For example, it is unclear whether the attorney handling the
284 matter has approached opposing counsel to try to ascertain whether he or she had, in fact,
285 received the client information and, if so, whether they are prepared to return it. Nor is the nature
286 or extent of the harm to the client's interest apparent. Clearly, the firm would have to take
287 reasonable measures to ascertain the relevant information and then take appropriate steps to
288 ameliorate the breach. If the breach was remediable and would not cause the client material
289 harm, no duty to disclose would arise. Correspondingly, if the breach was not remedial in the
290 sense that the information now in opposing counsel's possession gave it a significant advantage
291 in the litigation that it would not otherwise have, and if opposing counsel could not be
292 disqualified from further representing the opposing party, notice would have to be given.

293 [*alternative analysis*] The scenario involving Law Firm D, in contrast, is in flux and it is unclear
294 whether the misappropriation has compromised the client's interests and/or substantially
295 impaired the firm's ability to provide legal services. For example, it is unclear whether the
296 attorney handling the matter has approached opposing counsel to try to ascertain whether he or
297 she had, in fact, received the client information and, if so, whether they are prepared to return it.
298 Nor is the nature or extent of the harm to the client's interest apparent. Clearly, the firm would
299 have to take reasonable measures to ascertain the relevant information and then take appropriate
300 steps to ameliorate the breach. Nevertheless, even if the breach was remediable (for example, by
301 a successful motion to disqualify opposing counsel), the client would want to know that the firm
302 failed to perform a basic security precaution which jeopardized the representation, even if only
303 temporarily.

CLEAN

Attorney E'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.¹⁰ 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 laws and regulations such as HIPPA.¹¹

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 take reasonable steps 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. Fortunately, many, if

¹⁰ Affected clients might want or need to change passwords, modify or delete on-line accounts, and the like. 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.

¹¹ See <https://oag.ca.gov/system/files/LT%20Clients%20Sample%20w%20How%20To%201.pdf> for a notification letter from a California law firm flowing from a ransomware attack; HIPPA notification regulations: 45 CFR secs. 164.400-414

CLEAN

334 not most, of those steps are readily available and relatively easy to acquire and use. If the
335 unauthorized person uses them to harm the lawyer's clients, the failure to have taken reasonable
336 precautions is likely to harm the lawyer both professionally and financially.