

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

38 **Attorney B (she/her/hers)**

39  
40 At the end of a busy day, Attorney B meets a colleague for dinner at a restaurant. Waiting for her  
41 colleague to arrive, she checks her business and personal e-mail on her smartphone. B does not  
42 use a password, PIN, or biometric security feature.

43  
44 In the process of getting ready to go to bed, Attorney B suddenly realizes that she left her cell  
45 phone in the restaurant. She immediately calls the restaurant, but it is closed. B goes to the  
46 restaurant when it opens the next morning. The restaurant manager assures her that an employee  
47 saw the phone on the table, brought it to the manager, and that it was placed in a lost and found  
48 drawer from which he retrieves it.

49  
50 **Law Firm C**

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

63  
64 **Attorney D (they/them/their)**

65  
66 Attorney D is in-house counsel for a publicly traded pharmaceutical company that has been  
67 working on a cure for Alzheimer's disease. On vacation, Attorney goes to a coffee shop and  
68 accesses the shop's public Wi-Fi network to check their e-mail and conduct some personal  
69 business. Unknown to patrons or coffee shop staff, a hacker had set up a fake internet portal that  
70 resembled the one provided by the coffee shop. Attorney D doesn't realize that they actually  
71 logged on to that fake network. Attorney's laptop was not encrypted. Unbeknownst to Attorney  
72 D, the hacker sitting in the coffee shop with keystroke tracking software could see the text that  
73 people logged on to the fake network were typing on their laptops. The hacker read an e-mail  
74 that Attorney D wrote to the Company's marketing team which discussed a breakthrough on the  
75 Alzheimer's drug that was about to be publicly announced. The hacker immediately purchased  
76 stock in the company and made a large profit when the news was announced. The S.E.C.  
77 interviews company officials about the anomalous trade and the source of the information is  
78 revealed internally.

DISCUSSION

79  
80  
81  
82  
83  
84  
85  
86  
87  
88  
89  
90  
91  
92  
93  
94

**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 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.”<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>

95 **Introduction**

96 In COPRAC Formal Opn. 2015-193, we discussed attorneys’ ethical obligations when dealing  
97 with e-discovery, and in COPRAC Formal Opn. 2010-179 we discussed ethical issues arising  
98 from accessing client confidential information on a laptop over public wi-fi and a home wi-fi  
99 network. In both opinions, we adopted an approach that posed questions lawyers should consider  
100 in order to comply with the duties of competency and confidentiality. In light of the changing  
101 technology, we concluded that an on-going engagement with that evolving technology in the  
102 form of security issues to consider and re-consider was preferable to a “bright line” or  
103 categorical approach.

104  
105 This opinion extends that analysis to a broad range of cyber risks attendant on the use of  
106 electronic devices that contain client confidential information and connect to the internet and  
107 thus are theoretically accessible to anyone with an internet connection. We start with a useful  
108 description of data breaches: “A data event where material client confidential information is  
109 misappropriated, destroyed, or otherwise compromised, or where a lawyer’s ability to perform  
110 the legal services for which the lawyer is hired is significantly impaired by the episode.” ABA  
111 Formal Opn. 483 at p. 4 (2018) (hereafter ABA 483).

112  
113 **Confidentiality and Competency**

114  
115 The duty of competency (Rule 1.1) and the duty to safeguard clients’ confidences and secrets  
116 (Rule 1.6 and B&P Code sec. 6068(e)) require lawyers to make reasonable efforts to protect that  
117 information. The threshold requirement is for lawyers to have a basic understanding of the

---

<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>

## CLEAN

118 “benefits and risks associated with relevant technology.” COPRAC Formal Opn. 2015-193. This  
119 general principle requires lawyers to have a basic understanding of the risks posed using a given  
120 technology and, if necessary, obtain help from appropriate technology experts on assessing those  
121 risks and taking reasonable steps to prevent data breaches which potentially can harm clients.  
122 The threshold obligation to understand the risks is satisfied by learning where and how  
123 confidential information is vulnerable to unauthorized access. This inquiry must be made with  
124 respect to each type of electronic device as they have been or are incorporated into the lawyer’s  
125 practice.

126  
127 For example, computer systems can be breached by inadvertently clicking on a link in a  
128 seemingly legitimate “phishing” e-mail or text message or by installing an unvetted software app  
129 which can install malicious software on the system. Portable electronic devices can be accessed  
130 if security precautions such as passwords are missing or inadequate. Data on laptop computers  
131 can be accessed if the laptop is connected to a public network and if the data is not adequately  
132 protected. And the threats vary and widen as data thieves develop their attack strategies and as  
133 technologies develop.<sup>5</sup> Thus, lawyers must understand how their particular use of electronic  
134 devices and systems post risks of unauthorized access, they must be knowledgeable about the  
135 options available at any given point in time to minimize those risks, and they then must  
136 implement reasonable security measures in light of the risks posed. In addition, because law  
137 firms are frequent targets, firms ought to consider preparing a data breach response plan so that  
138 all stakeholders know how to respond when a breach occurs.<sup>6</sup>

139  
140 ABA 483 provides a useful list of competence-based duties that flesh out the requirement of  
141 “reasonable efforts” in handling confidential information in electronic form:

- 142
- 143 • The obligation to monitor for a data breach: “lawyers must employ reasonable efforts to  
144 monitor the technology and office resources connected to the internet, external data  
145 sources, and external vendors providing services relating to data and the use of data.” Id.  
146 at 5.
  - 147 • When a breach is detected or suspected, lawyers must “act reasonably and promptly to  
148 stop the breach and mitigate damage resulting from the breach.” Id. at 6. A preferable  
149 approach is to have a data breach plan in place “that will allow the firm to promptly  
150 respond in a coordinated manner to any type of security incident or cyber intrusion.” Id.  
151 at 6.
  - 152 • Investigate and determine what happened: “Just as a lawyer would need to assess which  
153 paper files were stolen from the lawyer’s office, so too lawyers must make reasonable  
154 attempts to determine whether electronic files were accessed, and if so, which ones. A  
155 competent attorney must make reasonable efforts to determine what occurred during the  
156 data breach.” Id. at 7.

157  
158 The duty to make reasonable efforts to preserve client confidential information do not create a  
159 strict liability standard. Nor does the duty “require the lawyer to be invulnerable or

---

<sup>5</sup> 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>.

<sup>6</sup> Discussed in ABA 483 at pp. 6-7 and in the ABA Cybersecurity Handbook.

160 impenetrable.” ABA 483 at p. 9. The precise nature of the security measures attorneys are  
161 expected to take depends on the circumstances. But, as the ABA has noted, “a legal standard for  
162 ‘reasonable’ security is emerging. That standard rejects requirements for specific security  
163 measures (such as firewalls, passwords, or the like) and instead adopts a fact-specific approach to  
164 business security obligations that requires a ‘process’ to assess risks, identify and implement  
165 appropriate security measures responsive to those risks, verify that the measures are effectively  
166 implemented, and ensure that they are continually updated in response to new developments.” Id.  
167 (quoting from the ABA Cybersecurity Handbook at 73).

168 “Reasonable efforts” are those which are reasonably calculated to eliminate, or at least minimize,  
169 particular, identified risks. For example, if a firm allows its staff to work on client matters  
170 remotely, it must ensure that all data flowing to and from those remote locations and the firm’s  
171 servers or cloud storage is adequately secured. The particular method or methods selected (VPN,  
172 encryption, etc.) will reflect the firm’s due consideration of the risks, the relative ease of use of  
173 different security precautions, time that would have to be spent training staff, and the like. Some  
174 security precautions are so readily available and user-friendly (such as the ability to locate and  
175 lock down portable devices in the event of loss or theft), that failure to implement them would be  
176 deemed unreasonable. Others will require a deeper assessment.

177 Finally, in law firms with subordinate lawyers, partners, particularly those with management  
178 responsibilities, should be aware of RPC rules 5.1 and 5.3. Rule 5.1 requires lawyers with  
179 “managerial authority in a law firm [to] make reasonable efforts to ensure that the firm has in  
180 effect measures giving reasonable assurance that all lawyers in the firm comply with these rules  
181 and the State Bar Act.” And Rule 5.3 makes this principle applicable to non-lawyer staff. Thus,  
182 part of the risk assessment process should include reasonable efforts to ensure that all firm  
183 members appreciate the risks involved in keeping confidential information on electronic systems  
184 and the steps that the firm’s managers have implemented to minimize the risk of unauthorized  
185 disclosure. Because the risk-assessment process is on-going, particularly with the introduction of  
186 new technologies and new threats, this duty would require subordinate lawyers and staff to be  
187 kept up to date on the firm’s evolving protective measures as they are implemented.

## 188 **Duty of Disclosure**

189 CRPC 1.4(a)(3) and B&P § 6068(m) require attorneys to keep their clients<sup>7</sup> reasonably apprised  
190 of any “significant developments” relating to the attorney’s representation of the client. Neither  
191 rule nor case law clearly define what events qualify as “significant.” (*See, e.g.*, Mark Tuft &  
192 Elaine Peck, *THE RUTTER GROUP GUIDE TO PROFESSIONAL RESPONSIBILITY*, § 6:128,  
193 acknowledging that what is “significant” under these provisions varies with each client’s needs  
194 and the nature of the representation.) Nevertheless, the authorities which have opined on the  
195 issue of whether the misappropriation, destruction, or compromising of client confidential  
196 information, or whether a cyber breach has significantly impaired the lawyer’s ability to provide  
197 legal services to clients is a “significant development” have concluded in the affirmative. *See*,  
198 *e.g.*, ABA 483 at 10; N.Y. State Bar Committee on Professional Ethics Opn. 842 (2010)  
199 (involving a data breach of a cloud storage provider); ABA Formal Opn. 95-398 (1995).

---

<sup>7</sup> 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.

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

207 **The Factual Scenarios:**

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

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

227 The situation of Law Firm C involves a common entry point for hackers: malware attached to a  
228 seemingly legitimate e-mail, also referred to as "phishing."<sup>8</sup> Given the ubiquity of this method of  
229 gaining access, solo practitioners and firms must consider and implement reasonable precautions,  
230 such as staff and attorney training, protocols for handling in-coming e-mails, and the like. Law  
231 Firm C has certainly been inconvenienced by the cyber breach, but the firm has confirmed that  
232 none of its clients were actually or potentially harmed because no confidential information was  
233 accessed, and the delay did not impair the firm's attorneys from continuing to provide necessary  
234 legal services to its clients. Therefore, the firm would not be required to disclose the incident. On  
235 the other hand, if the consultant could not preclude actual or potential unauthorized access, a risk  
236 of client harm remains and disclosure would be required.

---

<sup>8</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. 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

237 Attorneys who keep confidential information on their portable devices ought to be aware that  
238 accessing public Wi-Fi may open another access point for hackers. This is illustrated by Attorney  
239 D’s exposing confidential information to anyone with the capability of electronically  
240 “eavesdropping” on the Attorney’s keystrokes. Attorneys who work on client matters remotely  
241 (that is, on portable devices) must consider the risks of harm and take reasonable precautions, as  
242 discussed above, to prevent unauthorized disclosure. COPRAC Formal Opn. 2010-179 at 6  
243 (discussing use of laptop in unsecured and secured settings). Attorney D’s failure to secure their  
244 on-line communications exposed confidential information allowing a hacker to misappropriate  
245 and profit from that information. Regardless of whether the insider trading financially harmed  
246 the client, the misappropriation would constitute a significant development and require  
247 appropriate notice to the client. “[D]isclosure will be required if material client information was  
248 actually or reasonably suspected to have been accessed, disclosed or lost in a breach.” ABA 483  
249 at 14. Of course, the event would also require Attorney D to take appropriate remedial steps in  
250 terms of future on-line activities in unsecured locations.

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

252 In all cases of unauthorized access, disclosure to clients must be made immediately so the  
253 affected clients can take steps to ameliorate the harm. For example, affected clients might want or  
254 need to change passwords and modify or delete on-line accounts.<sup>9</sup> Given the importance of preserving  
255 client confidences, secrets and propriety information, it is appropriate to assume that reasonable  
256 clients would want to be notified if any of that information was acquired or reasonably suspected  
257 of being acquired by unauthorized persons.

258 With respect to the details of a required disclosure, “it must provide enough information for the  
259 client to make an informed decision as to what to do next, if anything. In a data breach scenario,  
260 the minimum disclosure required to all affected clients under Rule 1.4 is that there has been  
261 unauthorized access to or disclosure of their information, or that unauthorized access or  
262 disclosure is reasonably suspected of having occurred. Lawyers must advise clients of the known  
263 or reasonably ascertainable extent to which client information was accessed or disclosed. If the  
264 lawyer has made reasonable efforts to ascertain the extent of information affected by the breach  
265 but cannot do so, the client must be advised of that fact.” ABA 483 at p. 14. Lawyers may also  
266 have notification obligations under Cal. Civil Code sec. 1798.82 and federal and international  
267 laws and regulations such as HIPPA and the EU General Data Protection Regulation.<sup>10</sup>

268  
269  
270

## CONCLUSION

---

<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/>

## 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