# Two Recent ABA Ethics Opinions: More Law Firms Relying on the Cloud

by Sharon D. Nelson, Esq. and John W. Simek



The ABA released ABA Formal Ethics Opinion 482*, Ethical Obligations Related to Disasters*, on September 19, 2018. The opinion may be found at https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_opinion_482.authcheckdam.pdf. In the opinion, the Standing Committee on Ethics and Professional Responsibility clarifies the ethical obligations attorneys face when disaster strikes.

Lawyers must follow the duty of communication required by Rule 1.4 of the ABA Model Rules of Professional Conduct, which requires lawyers to communicate regularly with clients and to keep clients reasonably apprised of their cases. Following a disaster, a lawyer must evaluate available methods to maintain communication with clients. The opinion instructs that lawyers should keep electronic lists of current clients in a manner that is "easily accessible." Most lawyers have taken that to mean that the lists should be stored in the cloud so they can access them from an internet connection anywhere.

Lawyers should pay attention to the duty of competency, Rule 1.1, which includes a technology clause that requires lawyers to consider the benefits and risks of relevant technology. Because a disaster can destroy lawyers' paper files, lawyers "must evaluate in advance storing files electronically" so that they can access those files after a disaster. Storing client files through cloud technology requires lawyers to consider confidentiality obligations. Again, the opinion has been read by lawyers to encourage cloud storage.

With a little due diligence, this should not present much of a problem. We constantly encourage lawyers to keep backups in the cloud. It is prudent to have a local backup, but the cloud provides additional security. As we learned from Katrina, having a backup at the office and one at home a mile away is not sufficiently protecting confidential data.

If a disaster causes the loss of client files, lawyers must also consider their ethical obligations under Rule 1.15, which requires lawyers to safeguard client property. For current clients, lawyers can first attempt to reconstruct files by obtaining documents from other sources. If they cannot, lawyers must notify the clients of the loss of files or property. To prevent such losses, "lawyers should maintain an electronic copy of important documents in an off-site location that is updated regularly." Yup, we're back to the cloud again.

A disaster could impact financial institutions and, therefore, client funds. Thus, lawyers "must take reasonable steps in the event of a disaster to ensure access to funds the lawyer is holding in trust." It struck us that this could be highly problematic in some circumstances, but of course it is wise to do whatever one can.

A disaster may cause an attorney to have to withdraw from a client's case under Rule 1.16. "In determining whether withdrawal is required, lawyers must assess whether the client needs immediate legal services that the lawyer will be unable to timely provide," the opinion notes. We certainly saw a lot of withdrawals after Katrina. Entire law practices closed their doors, some forever.

The opinion also warns lawyers that they should not take advantage of disaster victims for personal gain: "Of particular concern is the possibility of improper solicitation in the wake of a disaster." Ambulance chasers, hurricane and flooding chasers – all distasteful, but they've been with us for a long time.

On balance, the opinion provides some good guidance and may help lawyers to form an incident response plan that complies with the guidance of this opinion. It's worth taking a look at your incident response plan to see if modifications are warranted. And if you don't have a formal incident response plan, this is a good time to formulate one! At a recent CLE with some 40+ attendees, only a single attendee had a written incident response plan. We need to do better than that – put that high on your agenda for 2019.

On October 17, 2018, the ABA issued Formal Opinion 484, *Lawyers' Obligations After an Electronic Data Breach or Cyberattack* which may be found at https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_op_483.pdf.

This opinion builds on the standing committee's Formal Opinion 477R released in May 2017, which set forth a lawyer's ethical obligation to secure protected client information when communicating digitally.

The new opinion states: "When a breach of protected client information is either suspected or detected, Rule 1.1 requires that the lawyer act reasonably and promptly to stop the breach and mitigate damage resulting from the breach."

The ethics opinion implicates Model Rule 1.1 (competence), Model Rule 1.4 (communications), Model Rule 1.6 (confidentiality of information), Model Rule 1.15 (safekeeping property), Model Rule 5.1 (responsibilities of a partner or supervisory lawyer) and Model Rule 5.3 (responsibilities regarding nonlawyer assistance).

There is a "rule of reason" overtone to the opinion, which states, "As a matter of preparation and best practices, however, lawyers should consider proactively developing an incident response plan with specific plans and procedures for responding to a data breach. The decision whether to adopt a plan, the content of any plan and actions taken to train and prepare for implementation of the plan should be made before a lawyer is swept up in an actual breach."

This is of course what cybersecurity experts have said for a very long time – and, in our experience, all large firms tend to have an incident response plan. The smaller firms? Not so much.

The opinion also recommends, in a footnote, that firms should have data retention policies that limit their possession of personally identifiable information. We certainly agree with that. Lots of firms have "zombie" data – data they don't know they have until there is a data breach.

Since data breaches cannot entirely be avoided, the opinion says, "When they do (have a breach), they have a duty to notify clients of the data breach under Model Rule 1.4 in sufficient detail to keep clients 'reasonably informed' and with an explanation 'to the extent necessary to permit the client to make informed decisions regarding the representation."

In general, when it comes to solo/small/midsize firms, virtually all experts agree that the cloud will protect confidential data better than law firms will. Their security expertise far exceeds that of the average law firm, their IT employees or their outside consultants. What questions to ask your cloud provider is the subject of a separate article. Maybe next time!

Taken together, the two opinions offer sound guidance – but it was particularly interesting to see what seems to be an increasing endorsement of cloud computing in Formal Ethics Opinion 482 as part of the solution to business continuity and the protection of confidential data.

*The authors are the President and Vice President at Sensei Enterprises, Inc., a digital forensics, information security and legal technology firm based in Fairfax, VA. 703-359-0700 (phone) 703-359-8434 (fax*) sensei@senseient.com, http://www.senseient.com.