Disasters and Data Breaches: The ABA Speaks

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

DID THE PARADE PASS YOU BY?

In 2018, the ABA released two very significant ethical opinions. One was Formal Opinion 483: Lawyers' Obligations After an Electronic Data Breach or Cyberattack (October 17, 2018). The other was Formal Opinion 482: Ethical Obligations Related to Disasters (September 19, 2018).

To our surprise, we rarely find CLE attendees who are aware of these opinions. Even those who are aware of them do not seem to know their details or understand their implications. Hence the inspiration for this article. Both opinions should be carefully read by lawyers seeking to understand their ethical duties in the event of a disaster (natural or man-made) or a data breach (which is of course a very specific form of a disaster)!

DATA BREACHES AND HEADLESS CHICKEN MODE

In our line of work, we see a lot of law firms who have been breached. "Headless Chicken Mode" is our name for the reaction of those who have not prepared for a breach – they have no incident response plan. They run in circles, hysterical, with no idea what to do. Sadly, there are a lot of law firms without an incident response plan –a 2018 study by IBM Resilient and the Ponemon Institute revealed that half of all organizations described their incident response plans as informal, ad hoc, or completely non-existent.

Today, for law firms, not having a formal incident response plan is inexcusable – and unethical under these new opinions. With respect to cyberattacks, our own experience has shown:

- The faster you catch a cyberattack, the less it will cost you and the faster you can recover.
- You are no stronger than your weakest link (usually your employees).
- With a good incident response plan, preparation is 2/3 of the effort, and the remaining 1/3 is solving the problems when an attack occurs.

THE CLOUD IS YOUR FRIEND

Whether you have a data breach or another form of disaster, the cloud is your friend. Opinion 482 talks about the duty of communication required by Rule 1.4, which requires lawyers to communicate regularly with clients and keep their clients reasonably apprised about 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."

The opinion also references Rule 1.1, which requires lawyers to consider the benefits and risks of relevant technology. It also notes that lawyers "must evaluate in advance storing files electronically" such they can access them after a disaster.

If your office is flooded (and maybe your home where you leave your backups), the best way to access client contact information is via the cloud. More and more, ABA opinions are not so gently pushing law firms toward the cloud. We agree completely that essential law firm data should, at the very least, be backed up in the cloud. Keep your data on premise if you like with an on premise backup, but make sure there is a copy in the cloud. Today, that is just a common sense precaution and almost universally accepted by legal technologists.

Yes, you need a reputable cloud provider, and you need to read the Terms of Service and ask questions regarding the security of client data, but there are many acceptable and respected cloud providers available to lawyers today – the fear of the cloud has faded. In fact, law firms tend to fear NOT being in the cloud.

SAFEGUARDING CLIENT PROPERTY

There was a time – and not so long ago – where lawyers obeyed Rule 1.15 (safeguarding client property) by locking up paper files. It is a whole new world today. If client data is destroyed, the opinion says lawyers can attempt to reconstruct files by obtaining documents from other sources. If they cannot, they must notify the clients of the loss of the files. 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.

In many law firms, cloud backups are updated as frequently as every 15 minutes. While that may not be ethically required, most firms at least perform daily cloud backups.

MONEY, ATTORNEY WITHDRAWAL AND GREED

As we saw with Katrina in particular, disasters can impact financial institutions and, therefore, client funds. Thus, the opinion says that lawyers "must take reasonable steps in the event of a disaster to ensure access for funds the lawyer is holding in trust." This largely presupposes that you are doing electronic banking, which most firms are, and can therefore access client funds once you have an internet connection (which means you need a redundant internet connection). You may also need to have another trusted signatory or, if the worst happens, have a successor lawyer to wind up your practice. Gloomy thoughts, but it's like having a will – simply a necessity of life and your profession.

In a true disaster, you may not be able to perform legal services and may have to withdraw. 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." Again, we harken back to Katrina, where many lawyers were forced by circumstances to withdraw from representation. Needless to say, you must seek the court's permission to withdraw as required by law and court rules. A good practice tip is to address in your engagement letter how to contact you in the event of a disaster.

When the U.S. Virgin Islands firm Bolt Nagi lost its St. Thomas office during Irma and Maria, our friend and colleague Tom Bolt had the law firm website temporarily altered to display his cell phone number. Tom, the firm's managing partner, certainly went the extra mile to make sure firm clients could contact him.

Many people seek to gain from disaster victims. The opinion 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." While the warning is well taken, the authors note anecdotally that they were never prouder of the legal profession than after Katrina, when so many lawyers and legal professionals reached out to help lawyers (and their clients) impacted by the flood waters of Katrina.

PRACTICING IN OTHER STATES

On this issue, you should read the opinion itself carefully. If you are displaced from your jurisdiction and seek to practice elsewhere temporarily, in accordance with Rule 5.5(c), you must obtain approval from the new jurisdiction.

The opinion cites a key provision of the ABA Model Court Rule on Provision of Legal Services Following Determination of Major Disaster. That rule provides in part that a lawyer displaced by a disaster "may provide legal services in this jurisdiction on a temporary basis if permitted by order of the highest court of the other jurisdiction."

Many lawyers simply want to volunteer to help disaster victims. The opinion states that, "Out-of-state lawyers may provide representation to disaster victims in the affected jurisdiction only when permitted by that jurisdiction's laws or rules, or by order of the jurisdiction's highest court."

The ABA Model Court Rule on Provision of Legal Services Following Determination of Major Disaster requires that "the supreme court of the affected jurisdiction must declare a major disaster and issue an order that allows lawyers in good standing from another jurisdiction to temporarily provide pro bono legal services in the affected jurisdiction through a nonprofit bar association, pro bono program, legal services program or other organization designated by the courts."

Just make sure you follow the rules. It is also helpful to volunteer your time through the ABA or other pro bono services providers. A good many of our ABA colleagues went down to New Orleans to help lawyers reestablish their practices. Even from Virginia, we took five Tulane Law School students under our wings and purchased/configured new laptops for them, which they took to Georgetown, which generously allowed them to continue their legal education there.

There is always a way to help without getting yourself in ethical trouble!

THE MOST LIKELY DISASTER: A DATA BREACH

The Cyber Readiness Report 2019, commissioned by global insurer Hiscox, found that 61% of global firms have been breached in the past year. While not specific to law firms, that is a dramatic increase – and law firms are by no means immune. It fact, we are a target-rich environment because we hold the data of so many

clients. And, to be frank, law firm security remains weak, especially in solo/small/midsized firms.

Data breaches are silent and deadly – not at all like the disasters recounted above. If you want to feel your blood pressure rise, Google “FireEye Live Cyber Threat Map” and watch the attacks in real time. In the last several years, we have witnessed cyberattacks routinely conducted by bots and seen attacks powered by artificial intelligence.

THE ABA SPEAKS TWICE IN TWO YEARS ON CYBERSECURITY

The ABA’s Formal Opinion 483, "Lawyers' Obligations After an Electronic Data Breach or Cyberattack" builds on the Standing Committee on Ethics and Professional Responsibility’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 opinion discusses 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). Where we have gone through these rules with respect to Opinion 482, we will not repeat ourselves here unless there are additional aspects to cover.

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."

Wait – didn’t we say that earlier in the article? In fairness, this is what all 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. No one is saying that a law firm need to be invincible because that is not possible. As the opinion states, "the potential for an ethical violation occurs when a lawyer does not undertake reasonable efforts to avoid data loss or to detect cyber-intrusion, and that lack of reasonable effort is the cause of the breach." There you have it in a nutshell.

ZOMBIE DATA

Is there anything not somehow affiliated with Zombies these days? For those of you not familiar with the term, zombie data is also known as "dark data," – data you don't know you have until after you have a data breach. The opinion takes a "throw out the trash approach" and recommends, in a footnote, that firms should have data retention policies that limit their possession of personally identifiable information. What you don't have can't hurt you.

As an aside, zombie data pops up all the time in e-discovery and causes a huge amount of expense, not to mention the negative effects it can have on a case when it is suddenly discovered. If you don't need it, and are not legally required to preserve it, get rid of it!

COMMUNICATING DATA BREACHES WITH CLIENTS

Since data breaches cannot entirely be avoided, the opinion says, "When a lawyer knows or reasonably should know a data breach has occurred, the lawyer must evaluate notice obligations. Model Rule 1.4. Rule 1.4(a)(3) provides that a lawyer must "keep the client reasonably informed about the status of the matter." Rule 1.4(b) provides: "A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation."

First, law firms must halt the attack, mitigate the damage and then make reasonable efforts to assess the data that may have been exposed. Not so easy. You can contract ransomware which exfiltrates your data before encrypting your files (therefore a data breach) or ransomware which only encrypts your files and then asks a ransom for the decryption key (therefore not a data breach). The opinion notes that your efforts in determining what happened and fixing it may be through qualified experts.

If you need to report an incident to a government agency, you are still bound by Rule 1.6. We sense there may be some tension over trying to report and trying to

maintain client confidential data. How do you know if the disclosure is "impliedly authorized?" Read the opinion fully to understand all the nuances of this dilemma.

Under Rule 1.4, the opinion says bluntly that you must inform a current client of a data breach that impacts their material confidential information. Forgive us for how we say this, but this duty is often honored "in the breach." Typically, law firms say they have no evidence that the confidential information was accessed or used. It's often a rusty nail, but that's where they frequently hang their hat.

What exactly are you supposed to tell clients in your disclosure? The opinion is a little vague, saying that "the disclosure must be sufficient to provide enough information for the client to make an informed decision as to what to do next, if anything."

The opinion dodges a bit when it comes to former clients, finding no duty to notify former clients unless there is something mandating notification.

FINAL WORDS

These are good opinions, worthy of a careful read. As is now customary with all opinions dealing with technology, modification of these opinions may need to be made over time. The two opinions are good roadmaps – and we hope many law firms who are woefully unprepared for disasters, including data breaches, use them as intended to prepare for the worst before it happens.

Sharon D. Nelson, Esq. is a practicing attorney and the president of Sensei Enterprises, Inc. She is a past president of the Virginia State Bar, the Fairfax Bar Association and the Fairfax Law Foundation. She a co-author of 17 books published by the ABA. snelson@senseient.com.

John W. Simek is vice president of Sensei Enterprises, Inc. He is a Certified Information Systems Security Professional and a nationally known expert in the area of digital forensics. He and Sharon provide legal technology, cybersecurity and digital forensics services from their Fairfax, Virginia firm. jsimek@senseient.com.