IT'S A BRAVE NEW WORLD OUT THERE

The Emerging Duty of Technological Competence

By John G. Browning

In 2012, a sea change occurred in the legal profession, particularly for those who came of age in the "good old days" when being competent in representing one's clients meant staying abreast of recent case law and statutory or code changes in one's area of concentration. In August 2012, the American Bar Association (ABA) — following the recommendations of its Ethics 20/20 Commission — formally approved a change to the Model Rules of Professional Conduct to make it clear that lawyers have a duty to be competent not only in the law and its practice, but in technology as well. Specifically, the ABA's House of Delegates voted to amend Comment 8 to Model Rule 1.1, which deals with competence, to read as follows:

> **Maintaining Competence.** To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology*, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.[1]

Now, of course, the ABA Model Rules are precisely that — a model. They provide guidance to states in formulating their own rules of professional conduct, and each state is free to adopt, ignore or modify the Model Rules. For a duty of technology competence to apply to lawyers in a given state, that state's particular rule-making body (usually the state's highest court) would have to adopt it.

Since 2012, 36 states have adopted the duty of technology competence by formally adopting the revised comment to Rule 1.1. In Louisiana, it was approved by the Louisiana Supreme Court on April 11, 2018, and was referenced via Public Ethics Opinion on Feb. 6, 2019.

For some of these states, even before the formal adoption of a technology competence requirement, there were clear indications that lawyers would be held to a higher standard when it came to technology impacting the practice of law. For example, in a 2012 New Hampshire Bar Association ethics opinion on cloud computing, the Bar noted that "competent lawyers must have a basic understanding of the technologies they use. Furthermore, as technology, the regulatory framework, and privacy laws keep changing, lawyers should keep abreast of these changes."[2]

Even the one state that has not adopted the ABA Model Rules, California nevertheless acknowledges the importance of technology competence. In a 2015 formal ethics opinion on e-discovery, the California Bar made it clear that it requires attorneys who represent clients in litigation either to be competent in e-discovery or to get help from those who are competent. Its opinion even expressly cited ABA's Comment 8 to Rule 1.1, stating, "Mandatory learning and skill consistent with an attorney's duty of competence includes 'keeping abreast of changes in the law and its practice, including the benefits and risks associated with technology.'"[3]

Louisiana was actually ahead of the curve in calling for tech competency. In 2005, an appeal from the 1st Circuit was part of a national wave of cases ushering in a "duty to Google." In *Weatherly v. Optimum Asset Mgmt. Inc.*, there was a dispute over the invalidation of a tax sale, with the mortgagee (Dr. Weatherly) alleging he hadn't received notice of the proceedings.[4] The mortgagor alleged that service by publication had been adequate, since the out-of-state Weatherly was not "reasonably identifiable." The trial court itself ran an Internet search, located Weatherly and concluded that he was indeed "reasonably identifiable" and voided the tax sale. The appellate court affirmed, holding that the trial judge's online search was not an abuse of discretion and that the mortgagor's failure to make use of online search tools did not constitute "reasonably diligent efforts."

Recent disbarments of Louisiana attorneys for online activities have revealed a disconnect on the part of some lawyers between their conduct on Internet and social media platforms and their ethical obligations as attorneys. In June 2015, the Louisiana Supreme Court disbarred then 52-year-old Joyce McCool for using Twitter and an online petition to engage in what it called a "social media blitz" against two judges presiding over child custody cases.[5] Upset with these judges' rulings, McCool had posted on social media what the Court described as many "false, misleading, and inflammatory statements," including accusing the judges in question of refusing to admit audio recordings of children talking about alleged abuse. McCool circulated an online petition calling for the judges' removal and solicited others to make ex parte contact with the judges (and with the state Supreme Court) to express their feelings about these sealed domestic proceedings. On one day alone (Aug. 16, 2011), McCool sent 30 tweets about the case and online petitions, including ones that indicated an awareness of the potential consequences of her actions: "I am SO going 2 have 2 change jobs after this. . . ! I'm risking sanctions by the LA supreme court; u could be a HUGE help."[6] In ordering McCool's disbarment, the Court found that the social media campaign she launched was "part of a pattern of conduct intended to influence the judges' future rulings in pending litigation," and that her actions "threaten[ed] the independence and integrity of the judicial system, and caus[ed] the judges concern for their personal safety and well-being."[7]

More recently, the Louisiana Supreme Court disbarred another attorney for online misconduct. On Dec. 5, 2018, the Court ordered the disbarment of former federal prosecutor Salvador (Sal) Perricone for posting anonymous online comments about pending investigations and cases being handed by himself or the U.S. Attorney's Office. The Court found that Perricone's "caustic, extrajudicial comments about pending cases strikes at the heart of the neutral dispassionate control which is the foundation of our system," and said its decision "must send a strong message . . . to all members of the bar that a lawyer's ethical obligations are not diminished by the mask of anonymity provided by the internet.[8] Between November 2007 and March 2012, using online pseudonyms like "Henry L. Mencken 1951," Perricone had posted more than 2,600 comments on nola.com (the website of the New Orleans *Times-*

Picayune). These comments included references to a defense lawyer who had "screwed his client" in a case Perricone was prosecuting as well as commentary about the prosecution of New Orleans police officers in the Danziger Bridge shootings of six civilians (saying of the officers involved that "NONE of these guys should have ever been given a badge").[9]

Not surprisingly, given the McCool and Perricone episodes, the Louisiana State Bar Association (LSBA) issued a newly updated Code of Professionalism in October 2018, with new amendments including a vow to use "technology, including social media, responsibly." In February 2019, the LSBA formally addressed the issue of tech competence with the issuance of an ethics opinion, "Lawyer's Use of Technology."[10] The opinion acknowledged that "technology and the Internet can modify the way a lawyer practices, affecting communication, practice management, handling evidence and data storage," before concluding, "a lawyer must consider the benefits and risks associated with using technology in representing a client." En route to that conclusion, the opinion identified the Louisiana Rules of Professional Conduct most likely to be implied by a lawyer's use of technology, including Rules 1.1(a) (competent representation); 1.3 (acting with reasonable diligence); 1.4 (communicating with a client); 1.6 (maintaining confidentiality); 1.15(a) (safeguarding a client's property); and 5.3 (supervision of nonlawyers employed by or associated with the lawyer).

The opinion notes that whether it was a natural disaster like Hurricane Katrina or cybersecurity risks like computer hacking or data breach events, part of a lawyer being competent and diligent is using appropriate technology to safeguard a client's information (like maintaining backup systems). In addition, because use of technology may involve working with nonlawyer employees or contractors (such as in the areas of cloud storage or e-discovery vendors), the opinion reminds lawyers that they are responsible for ensuring that such nonlawyers' conduct lives up to the lawyer's ethical standards.

And in communicating with clients and maintaining confidentiality, this ethics opinion cautions that attorneys must take into consideration the particular security needs of each client as well as the dangers of inadvertent disclosure of information due to email "web bugs," email "opens" and "forwards," and other risks.

What consequences does this sea change hold for Louisiana practitioners? First, you don't have to go from Luddite to Geek Squad member; just understand the basics of the technology you use, and become conversant in how it can impact your practice as well as how it functions. This includes law practice management technology, such as email and document creation and document management software. It also can include things like e-discovery and technology-assisted review (TAR) for litigators. With use of filesharing sites like Dropbox and Box becoming commonplace, lawyers have to be conversant in cloud computing and the ethical questions its use raises. With cybersecurity's importance for both law firms and the clients they serve, basic working knowledge of cybersecurity measures (such as encryption for confidential communications) and risks like ransomware and phishing schemes are a vital part of being tech competent. For example, the most recent opinion from the ABA Standing Committee on Ethics and Professional Responsibility, which called for lawyers to use "reasonable efforts" (such as encryption) to ensure that communications with clients are secure, highlighted how these efforts spring from not only the ethical duty to preserve client confidences but also the duty of competence as well.[11] It states that a lawyer must "act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision."[12]

Perhaps the best way to illustrate the mistakes lawyers need to avoid making when it comes to these newly raised standards of technology competence is to share some cautionary tales about lawyers whose lack of tech competence led to disciplinary problems, court sanctions and even malpractice exposure. Some of the following examples may provoke a "but I would never do that" reaction, while others may fall under the category of "thus but for the grace of God go I." All of them, however, demonstrate the dangers of not living up to technology competence standards.

CAUTIONARY TALES OF THE CONSEQUENCES OF TECH INCOMPETENCE

DON'T BLAME THE SPAM FILTER

In *Emerald Coast Utilities Auth. v. Bear Marcus Pointe, L.L.C.*, a Florida appellate court administered a tough lesson for the Pensacola law firm of Odom & Barlow: Keep your email system's spam filter up to date or risk the consequences.[13] Odom & Barlow was counsel to Emerald Coast in an eminent domain case. On March 18, 2014, the trial court rendered judgment granting approximately $600,000 in attorney fees to Bear Marcus, starting the clock running on a 30-day window to appeal the ruling. Emerald Coast's lawyers missed the deadline but filed a May 12, 2014, motion for relief, citing Florida Rule of Civil Procedure 1.540(b) which gives courts discretion to set aside final judgments in cases due to "mistake, inadvertence, surprise or excusable neglect." They claimed they had not received the email within their system.

The court engaged in extensive fact-finding, and the picture that emerged was not a flattering one for Odom & Barlow. The IT director for the Clerk of Court retrieved logs from the clerk's e-service system, showing that emails containing the order were sent to both primary and secondary emails designated by the firm on March 20, 2014, and that there were no error messages or bouncebacks indicating that the email had not been delivered. Another witness, from an independent consulting firm, reviewed the email log printouts and examined the servers and work stations at the firm. While he found no evidence of destruction of the emails, he conceded that it was "fairly unusual for a company to configure their system to not create any email logs," and that, if it had, he could have had complete logs to determine if the server had received the emails in question.[14] Some of the most damning testimony came from Odom & Barlow's own IT consultant who had provided services to the firm since 2007. He confirmed that the firm's email filtering system was configured to drop and permanently delete emails perceived to be spam without alerting the recipient that email was deleted. The IT consultant further testified that he had advised the firm on the danger of this spam filtering due to the risk of legitimate emails being identified as spam. He had recommended a vendor to the firm to handle spam-filtering, but the firm rejected this recommendation because it "did not want to spend the extra money."[15]

Even the opposing counsel at Fixel & Willis got in a few jabs, describing their protocol to cover email loopholes. The firm assigned a paralegal to check the court's website every three weeks in order to catch and respond to any posted orders. The appellate court was not sympathetic to Odom & Barlow's plight either. It affirmed the trial court's ruling that the firm's misplaced reliance on its questionable email system did not constitute excusable neglect. The court held that the firm "made a conscious decision to use a defective email system without any safeguards or oversight in order to save money."[16] On rehearing, the appellate court reiterated its reasoning, concluding that "Counsel has a duty to have sufficient procedures and protocols" in place, including "use of an email spam filter with adequate safeguards and independent monitoring."[17] With the passage of time on appeal, the attorney fee award at issue had grown to more than $1 million.

KNOW WHETHER YOUR REDACTION IS REALLY REDACTED

It can be both embarrassing and damaging to one's case to produce "redacted" documents that aren't actually redacted. In 2017, lawyers at the Department of Justice (DOJ) learned —thanks to an alert *Law360* reporter — that the redactions they made in a motion hadn't been properly redacted. The case was a high-profile Libor-rigging case against a former Deutsche Bank trader, Gavin Black, in which protected testimony was included (in redacted form) in a motion filed in federal court in New York. But during the roughly 12 hours that the document was publicly viewable in its original form, it was apparent that the redactions hadn't been done properly. "One sentence was highlighted in black and written in a gray font that was clearly legible," while other portions that had been blocked out "were easily read by copying and pasting the contents of the brief into another text document" and word searches returned "text that was barely hidden behind the faulty redactions."[18] A DOJ spokesperson blamed the improper redactions on "a technical error in the electronic redaction process," but clearly the error was, in fact, human. Quick tip: To test whether a document is properly redacted, highlight the redacted portion, copy it and paste it into a document and see if the underlying text still appears.

TECHNOLOGICAL INCOMPETENCE IN E-DISCOVERY IS NO EXCUSE (PART I)

In *James v. National Financial, L.L.C.*, the Delaware Court of Chancery was not sympathetic to the lead defense counsel's explanation for failures to produce requested electronically stored information — the explanation was that he was "not computer literate."[19] The case involved class action claims against a payday loan lender for violating the Delaware Consumer Fraud Act as well as the federal Truth in Lending Act. National Financial had been ordered to produce electronically

stored information about each of its loans between September 2010 and September 2013. After multiple deficient discovery responses, and several court orders, the court's patience was at an end, and it sanctioned the defense with both deemed admissions as well as monetary sanctions. But it also turned a deaf ear to defense counsel's protests that "I am not computer literate. I have not found presence in the cybernetic revolution . . . This was out of my bailiwick." Pointing out that "technological incompetence is not an excuse for discovery misconduct," the court reminded counsel that technological competence was specifically included in Rule 1.1 of the Delaware Lawyers' Rules of Professional Conduct. It further stated that "deliberate ignorance of technology is inexcusable . . . If a lawyer cannot master the technology suitable for that lawyer's practice, the lawyer should hire tech-savvy lawyers tasked with responsibility to keep current, or hire an outside technology consultant."[20]

TECHNOLOGICAL INCOMPETENCE IN E-DISCOVERY IS NO EXCUSE [PART II]

Even if you are not the sharpest knife in the drawer when it comes to e-discovery, what is the worst that can happen? A sanctions order, perhaps, or maybe an unhappy client? Try one of the biggest data breaches of the year.

New Jersey lawyer Angela Turiano was outside counsel for Wells Fargo and Steven Sinderbrand, one of its financial advisers, in a defamation lawsuit brought by Gary Sinderbrand, also a Wells Fargo adviser. In his case, Gary sought third-party discovery from Wells Fargo, including emails between Steven and the bank. In response to the subpoena, Wells Fargo agreed to conduct a search of certain custodians' email accounts using designated search terms. Using a third-party vendor's e-discovery software, Turiano reviewed what she believed was the entire universe of potentially relevant information and excluded privileged documents and nonresponsive information. She also conducted a "spot check" of the production, before placing the information on an encrypted CD marked "confidential" and providing that CD to opposing counsel. Unfortunately, because she did not understand the software's functionality, she wound up producing documents that had not been reviewed by her for confidentiality and privilege.[21] In addition, documents that she had flagged as needing redactions were not redacted before production. The result was the production of "a vast trove of confidential information" about tens of thousands of Wells Fargo's wealthiest clients, revealing billions of dollars of client account information from all over the United States and possibly Europe as well.[22] The 1.4 gigabytes of Wells Fargo files included customer names, Social Security numbers, the size of their investment portfolios, portfolio performance, mortgage details and other information — much of it about the bank's high net worth investors. One file, for example, was that of a hedge fund billionaire with at least $23 million in holdings with Wells Fargo.[23]

As bad as this was, Turiano found out when her opposing counsel disclosed the information to the *New York Times*. He also initially refused to return the inadvertently produced information, and Wells Fargo had to obtain court orders in New York and New Jersey to prevent its further dissemination. In the meantime, Wells Fargo had to contend with the adverse publicity and data breach notification obligations triggered by such an event. In an affirmation filed in court, Turiano acknowledged her colossal blunder, stating that she "misunderstood the role of the vendor," "may have miscoded some documents during my review," and that she "had not reviewed certain emails containing, or with attachments containing, Confidential Information."[24]

Turiano's mistake highlights the ethical risks as well as malpractice exposure that can accompany errors brought about by tech incompetence. Potential claims could include not just damages for potential claims made by the public, but also the costs that the client might incur such as legal fees for responding to the data breach and subsequent regulatory actions. It also underscores the importance of the guidelines delineated by the State Bar of California Standing Committee on Professional Responsibility and Conduct in its Formal Opinion No. 2015-193. In that opinion, lawyers engaging in e-discovery are directed to either become competent technologically, have other counsel or experts who have such competence, or refrain from handling such matters altogether.

TECHNOLOGICAL INCOMPETENCE CAN GET YOU DISBARRED

James Edward Oliver was a veteran bankruptcy practitioner in Oklahoma for 30 years, with a spotless disciplinary history. But, thanks to his admitted "lack of expertise in computer skills," he lost his right to practice before a bankruptcy court and received a public censure. Licensed since 1967, Oliver had practiced extensively and the Oklahoma Supreme Court even acknowledged that "no testimony nor any documents showed an insufficiency in Oliver's knowledge of substantive bankruptcy law." The problem, it seemed, was "technological proficiency."

Specifically, that meant e-filing. After Oliver failed repeatedly to properly submit documents electronically (even with assistance from court staff), Judge Sarah Hall of the U.S. Bankruptcy Court for the Western District of Oklahoma suspended him for 30 days. When he failed to show improvement, Judge Hall suspended him for another 60 days after directing Oliver to "have a lawyer on board" to help him. After Oliver failed to get such assistance and failed at nine "homework" documents that she told him to submit (error-free and without third-party assistance), Judge Hall permanently suspended Oliver on June 15, 2015, from practice before the Western District bankruptcy court, after finding that Oliver had paid another lawyer to "ghost write" his assignments.

When Oliver failed to report this discipline to the Oklahoma Bar, he wound

up in front of the Oklahoma Supreme Court. In its March 29, 2016, opinion, that Court imposed a public censure, and encouraged Oliver "to continue to improve his computer skills, or better, to hire an adept administrative assistant to do his pleadings." The dissent, however, took a harsher view, faulting Oliver for his "demonstrated incompetency to practice law before the bankruptcy court" and calling for a two year plus one day suspension.[25]

WHEN TECHNOLOGICAL COMPETENCE ALSO MEANS BEING AWARE OF CYBERSCAMS

Lawyers and law firms have been called the "soft underbelly" of business security due to their perpetual game of catch-up when it comes to cybersecurity. From law firms getting hacked (witness the "Panama Papers" case), or being victimized by viruses, data breaches, ransomware or other cyberintrusions, a law firm's commitment to cybersecurity is more important than ever. Moreover, failure to adopt reasonable cybersecurity measures can not only endanger client data, but it can trigger malpractice liability and disciplinary concerns. In an era rife with Internet scams, this also means lawyers who aren't tech savvy when it comes to scams are begging for ethics troubles.

Take, for example, Robert Allen Wright, Jr. In 2013, the Iowa Supreme Court suspended his license to practice law for at least a year. Wright, who was licensed in 1981 and who handled a general practice that included criminal and family law, came to believe that one of his criminal clients was the beneficiary of an $18.8 million bequest from a long-lost relative in Nigeria. All he needed, it seemed, was to pay the $177,000-plus in taxes, and the funds in Nigeria would be released. Not only was Wright taken in by this "Nigerian prince" Internet scam, he presented a number of his even more gullible clients with this "investment opportunity" in an attempt to come up with the money needed to pay the "taxes" in order to collect the "inheritance funds." Needless to say, neither Wright nor the clients from whom he had solicited funds ever saw their money again. The Iowa Supreme Court observed that "Wright appears to have honestly believed — and continues to believe — that one day a trunk full of . . . one hundred dollar bills is going to appear upon his office doorstep," and it also took note of the fact that Wright was not the first lawyer in Iowa or elsewhere to have fallen for a variation on this "Nigerian prince/inheritance" Internet scam. However, the Court found that, among other disciplinary violations, Wright's failure to do any Internet due diligence constituted a failure of his duty of competence under Iowa's rules. His license was suspended for a minimum of one year.[26]

CONCLUSION

The "new normal" of requiring lawyers to be tech competent encompasses much more than the mastery of substantive legal skills and knowledge that once defined "competent representation." In today's era of Google, Snapchat, Facebook, Twitter and cloud computing, lawyers must be knowledgeable of both the benefits and the risks of the technology that is out there, including the functionality of the technology they are actually using (or, in some cases, should be using). Doing so also involves a heightened appreciation for the importance of cybersecurity measures, such as using encryption for attorney-client communications. But a necessary first step, whether you are a dinosaur or a digital native, a Luddite or a thought leader, is education.

FOOTNOTES

1. ABA Model Rules of Prof. Conduct, Rule 1.1, Comment 8 (2012) (emphasis added).
2. New Hampshire Bar Ass'n, Advisory Op. 2012-13/4.
3. California State Bar Formal Op. No. 2015-193.
4. 2004-2734 (La. App. 1 Cir. 12/22/05), 928 So. 2d 118.
5. In re McCool, 2015-0284 (La. 6/30/15), 172 So.3d 1058.
6. *Id.* at 6, 172 So.3d at 1063.
7. *Id.* at 13, 172 So.3d at 1067.
8. In re Perricone, 2018-1233 (La. 12/5/18), 263 So.3d 309.
9. *Id.* at 6, 263 So.3d at 312.
10. LSBA Public Op. 19-RPCC-021 (Feb. 6, 2019).
11. ABA Formal Ethics Op. 477 (May 4, 2017).
12. *Id.*
13. Emerald Coast Utilities Auth. v. Bear Marcus Pointe, L.L.C., 227 So.3d 752 (Fla. 1st DCA 2017).
14. *Id.* at 754.
15. *Id.* The cost would have been $700-$1,200 annually.
16. *Id.*
17. *Id.*
18. Robert Ambrogi, "Stupid Lawyer Tricks: Legal Tech Edition," Above the Law (Oct. 16, 2017 1:02 PM), *https://abovethelaw.com/2017/10/stupid-lawyer-tricks-legal-tech-edition/.*
19. James v. Nat'l Fin., L.L.C., C.A. No. 8931-VCL (Dec. 5, 2014), 2014 WL 6845560.
20. *Id.* at *12.
21. Christine Simmons, "Lawyer's 'Inadvertent' E-Discovery Failures Led to Wells Fargo Data Breach," N.Y. Law J. (Oct. 14, 2017 2:02 a.m.), *https://www.law.com/newyorklawjournal/sites/newyorklawjournal/2017/07/26/lawyers-inadvertent-e-discovery-failures-led-to-wells-fargo-data-breach/?slreturn=20180127080210.*
22. *Id.*
23. Serge F. Kovaleski and Stacy Cowley, "Wells Fargo Accidentally Releases Trove of Data on Wealthy Clients," N.Y. Times (July 21, 2017), *https://www.nytimes.com/2017/07/21/business/dealbook/wells-fargo-confidential-data-release.html.*
24. Affirmation of Angela Turiano, Doc. No. 36, Mill Lane Mgmt., L.L.C. and Gary Sinderbrand v. Wells Fargo Advisors, L.L.C. and Steven Sinderbrand, Index No. 652025/2017, Sup. Ct. of N.Y. (July 24, 2017).
25. State ex rel. Oklahoma Bar Ass'n v. Oliver, 2016 OK 37, 369 P. 3d 1074. Oklahoma is not the only state to take a lawyer to task for incompetence in e-filing. In 2008, the Kansas Supreme Court suspended another bankruptcy lawyer for the same thing.
26. Iowa Supreme Court Attorney Disciplinary Bd. v. Wright, 840 N.W. 2d 295 (Iowa 2013).

John G. Browning is a partner in the Plano, Texas, office of Spencer Fane, L.L.P., where he handles civil litigation in state and federal courts. The author of four books and numerous articles on law and technology, he is an adjunct professor at three law schools and is the chair of the Computer and Technology Section of the State Bar of Texas. (jbrowning@spencerfane.com; Ste. 650, 5700 Granite Parkway, Plano, TX 75024)