University of Dayton Law Review

Volume 44 | Number 2 Article 3

3-1-2019

The New Duty of Digital Competence: Being Ethical and Competent in the Age of Facebook and Twitter

John G. Browning
Southern Methodist University

THE NEW DUTY OF DIGITAL COMPETENCE: BEING ETHICAL AND COMPETENT IN THE AGE OF FACEBOOK AND TWITTER

John G. Browning[*]

I. INTRODUCTION – IT'S A BRAVE NEW WORLD OUT THERE

In 2012, a sea change occurred in the legal profession,[1] particularly for those who came of age in the "good old days," when being competent in

* John G. Browning is a shareholder in the Dallas, Texas law firm of Passman & Jones, where he handles a wide variety of civil litigation in state and federal courts. The author of several books on social media and the law, he is an adjunct professor at SMU-Dedman School of Law.

[1] ABAComm'n on Ethics 20/20, Report to the House of Delegates Resolution 105A (2012), http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/2012_hod_annual_meeting_105a_filed_may_2012.authcheckdam.pdf

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.[2] Specifically, the ABA's House of Delegates voted to amend Comment 8 to Model Rule 1.1, which deals with Maintaining Competence, to read as follows:

> 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.[3]

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.

And since late 2012, more than half of the country has adopted the duty of technology competence by formally adopting the revised comment to Rule 1.1.[4] Twenty-eight states in all, have done this. The states, and the dates on which they did so, are as follows:

State	**Date**
Alaska	effective October 15, 2017
Arizona	effective January 1, 2015
Arkansas	approved June 26, 2014
Colorado	approved April 6, 2016
Connecticut	approved April 6, 2016

[2] MODEL RULES OF PROF'L CONDUCT r. 1.1 cmt. 8 (AM. BAR ASS'N 2012).
[3] *Id.*
[4] Tad Simons, *For a Lawyer, What does "Technology Competence" Really Mean?*, http://www.legalexecutiveinstitute.com/lawyers-technological-competence/ (last visited Feb. 23, 2019).

State	Date
Delaware	approved January 15, 2013
Florida	approved September 29, 2016
Idaho	approved March 17, 2014
Illinois	approved October 15, 2015
Indiana	approved October 15, 2015
Iowa	approved October 15, 2015
Kansas	approved January 29, 2014
Kentucky	approved November 15, 2017
Louisiana	approved by Louisiana Supreme Court April 11, 2018 and via Public Ethics Opinion February 6, 2019
Massachusetts	approved March 27, 2015
Minnesota	approved February 24, 2015
Missouri	approved September 26, 2017
Montana	via Bar petition and Supreme Court Order of September 22, 2016
Nebraska	adopted June 28, 2017
New Hampshire	approved November 10, 2015
New Mexico	approved November 1, 2013
New York	adopted March 28, 2015
North Carolina	adopted July 25, 2014
North Dakota	adopted December 9, 2015

State	Date
Ohio	approved February 14, 2015
Oklahoma	approved September 19, 2016
Pennsylvania	approved October 22, 2013
Tennessee	adopted March 6, 2017
Texas	adopted February 26, 2019
Utah	adopted March 3, 2015
Vermont	adopted October 9, 2018
Virginia	adopted December 17, 2015
Washington	approved June 2, 2016
West Virginia	approved September 29, 2014
Wisconsin	approved July 21, 2016
Wyoming	approved August 5, 2014

[5]

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 "[c]ompetent 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."[6]

[5] Bob Ambrogi, *Tracking Adoption of Tech Competence Rule: A New Home for My List of States*, LAWSITES (June 18, 2018), https://www.lawsitesblog.com/2018/06/tracking-adoption-tech-competence-rule-new-home-list-states.html. This list will soon include Michigan, whose Supreme Court has proposed adding technological competency to the list of required skills under the state's rules of professional conduct for attorneys. This proposal awaits adoptions by the Secretary of the State Bar and the State Court Administration of Michigan. *See* Keegan Boyle, *Michigan Supreme Court Proposes Changes to Attorney Rules in Light of New Technology*, JURIST (April 22, 2019), https://www.jurist.org/news/2019/04/michigan-supreme-court-proposes-changes-to-attorney-rules-in-light-of-new-technology/.

[6] N.H. Bar Ass'n, Advisory Op. 2012-13/4 (2013).

Even the one state that has not adopted the ABA Model Rules, California, nevertheless acknowledges the importance of technology competence.[7] In a 2015 formal ethics opinion on e-discovery (which will be discussed later),[8] the California Bar made it clear that it requires attorneys who represent clients in litigation to either be competent in e-discovery or to get help from those who are competent.[9] Its opinion even expressly cited ABA's Comment 8 to Rule 1.1, stating that "[m]aintaining 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.'"[10]

What consequences does this sea change hold for 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 e-mail, document creation, and document management software. It can also include things like e-discovery and technology assisted review ("TAR") for litigators. With use of file-sharing 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 technology competent. For example, the most recent opinion from the ABA Standing Committee on Ethics and Professional Responsibility called for lawyers to use "reasonable efforts" (such as encryption) to ensure that communications with clients are secure, and highlighted how these efforts spring from not only the ethical duty to preserve client's confidences but 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

---

[7] Steven M. Puiszis, A Lawyer's Duty of Technological Competence, https://www.americanbar.org/content/dam/aba/events/professional_responsibility/2017%20Meetings/Conference/conference_materials/session4_information_governance/puiszis_lawyers_duty_technological_competence.authcheckdam.pdf (last visited Feb. 23, 2019).

[8] Infra, sec. F.

[9] Cal. State Bar, Formal Op. 2015-193 (2015).

[10] *Id.*

[11] ABA Comm'n on Ethics & Prof'l Responsibility, Formal Op. 477 (2017).

[12] *Id.*

competence led to disciplinary problems, court sanctions, and even malpractice exposure. Some of the following examples may provoke the reaction "but I would never do that," while others may fall under the category of "there but for the grace of God go I." All of them, however, demonstrate the dangers of not living up to technology competence standards.

II. CAUTIONARY TALES OF THE CONSEQUENCES OF TECHNOLOGY INCOMPETENCE

A. Do Not Blame the Spam Filter

In *Emerald Coast Utilities Authority v. Bear Marcus Pointe, LLC*, a Florida appellate court administered a tough lesson for the Pensacola law firm of Odom & Barlow: keep your e-mail system's spam filter up-to-date, or risk the consequences.[13] Odom & Barlow were counsel to Emerald Coast in an eminent domain case.[14] On March 18, 2014, the trial court rendered judgment granting approximately $600,000 in attorneys' fees to Bear Marcus, starting the clock running on a thirty-day window to appeal the ruling.[15] 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."[16] They claimed they had not received the e-mail 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 Courts retrieved logs from the clerk's e-service system, showing that e-mails containing the order were sent to both primary and secondary e-mails designated by the firm on March 20, 2014, and that there were no error messages or bounce backs indicating that the e-mail had not been delivered.[17] Another witness from an independent consulting firm reviewed the e-mail log printouts and examined the servers and work stations at the firm.[18] While he found no evidence of destruction of the e-mails, 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 e-mails in question.[19]

---

[13] *See generally* Emerald Coast Util. Auth. v. Bear Marcus Pointe, LLC, 227 So. 3d 752 (Fla. Dist. Ct. App. 2017).

[14] *Id.* at 753.

[15] *Id.* Jim Little, *Spam Email Filter Could Cost ECUA Ratepayers Up $400,000 in Lawsuit*, PENSACOLA NEWS J. (Aug. 16, 2017), https://www.pnj.com/story/news/2017/08/16/spam-email-filter-could-cost-ecua-ratepayers-up-400-000-lawsuit/568387001/.

[16] *Id.* at 753, 756. Fla. R. Civ. P. 1.540(b).

[17] *Emerald Coast*, 227 So. 3d at 755.

[18] *Id.*

[19] *Id.* at 754.

Some of the most damning testimony came from Odom & Barlow's own IT consultant, who had provided services to the firm beginning in 2007.[20] He confirmed that the firm's e-mail filtering system was configured to drop and permanently delete e-mails perceived to be spam without alerting the recipient that the e-mail had been deleted.[21] The IT consultant further testified that he had advised the firm on the danger of this spam filtering due to the risk of legitimate e-mails being identified as spam.[22] 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."[23]

Even the opposing counsel at Fixel & Willis got in a few jabs, describing their protocol to cover e-mail loopholes.[24] The firm assigned a paralegal to check the court's website every three weeks in order to catch and respond to any posted orders.[25] The appellate court was not sympathetic to Odom & Barlow's plight either, affirming the trial court's ruling that the firm's misplaced reliance on its questionable e-mail system did not constitute excusable neglect.[26] The court held that the firm "made a conscious decision to use a defective e-mail system without any safeguards or oversight in order to save money."[27] On rehearing, the appellate court reiterated its reasoning, concluding that "[c]ounsel has a duty to have sufficient procedures and protocols in place," including "use of an e-mail spam filter with adequate safeguards and independent monitoring."[28] With the passage of time on appeal, the attorneys' fee award at issue had grown to over $1 million.[29]

B. More E-Mail Misadventures

Beware of "reply all," and be careful whom you carbon copy on an e-mail. That is the harsh lesson learned by Wilmer Cutler Pickering Hale & Dorr recently.[30] In September 2017, the *Wall Street Journal* published a report about the Securities and Exchange Commission's ("SEC") probe of PepsiCo's 2011 acquisition of a Russian beverage company, Wimm-Bill-Dann, and the 2012 departure of PepsiCo's general counsel, Maura Smith, in the midst of whistleblower claims. The *Wall Street Journal's* reporter had many details about the investigation, thanks to information (including a memo about Smith's subpoena by the SEC) "mistakenly sent by a WilmerHale

---

[20] *Id.*
[21] *Id.*
[22] *Id.*
[23] *Id.* at 757. The cost would have been $700–$1,200 annually. *Id.* at 754.
[24] *Id.* at 755.
[25] *Id.*
[26] *Id.* at 758.
[27] *Id.* at 757.
[28] *Id.* at 758.
[29] Little, *supra* note 15.
[30] Katelyn Polantz, Wilmer 'Inadvertently' Leaks Pepsi Client Secrets to Wall Street Journal, CORPORATE COUNSEL (Sept. 27, 2017, 1:17 PM), https://www.law.com/nationallawjournal/almID/1202799058944/Wilmer-Inadvertently-Leaks-Pepsi-Client-Secrets-to-Wall-Street-Journal-/.

attorney to a *Wall Street Journal* reporter as part of communication to other attorneys working on the matter."[31] The information included attorney-client privileged documents and attorney work product, including a 2012 memo prepared by Gibson Dunn & Crutcher lawyers who conducted an internal investigation critical of the Wimm-Bill-Dann deal[32] Wilmer Hale was quick to fall on its sword, stating "'[w]e deeply regret that privileged documents were inadvertently e-mailed to a reporter at the *Wall Street Journal*. Wilmer Hale takes full responsibility, and we apologize to our client. . . . We are taking additional measures designed to ensure that e-mails are not misaddressed to unintended recipients.'"[33]

C. Know Whether Your Redaction is Really 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 had not been properly redacted.[34] 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.[35] However, during the roughly twelve hours that the document was publicly-viewable in its original form, it was apparent that the redactions had not been done properly.[36] "'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.'"[37] A DOJ spokesperson blamed the improper redactions on "'a technical error in the electronic redaction process[,]'" but clearly the error was in fact human.[38] As a quick tip, it is always important to test whether a document is properly redacted by highlighting the redacted portion, copying it, and pasting it into a document to see if the underlying text still appears.

D. Know What You are Producing (and Admitting)

In *State v. Ratliff*,[39] the North Dakota Supreme Court considered whether the robbery and aggravated assault convictions, arising out of a 2012 home invasion, should be thrown out because a DVD of surveillance video footage of the incident also included (due to re-recording at the police station)

---

[31] *Id.*
[32] *Id.*
[33] *Id.*
[34] 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/.
[35] *Id.*
[36] *Id.*
[37] *Id.*
[38] *Id.*
[39] 849 N.W.2d 183 (N.D. 2014), *aff'd*, 882 N.W.2d 716 (N.D. 2016).

audio of law enforcement officers as they were making a copy of the surveillance video.[40] Noting that the audio was unintelligible, that it contained nothing prejudicial, and that defense counsel had not objected during the trial, the court affirmed the conviction.[41]

Significantly, however, the decision included a lengthy special concurring opinion by Justice Crothers, who took the opportunity to write about electronically stored information becoming more and more significant as a source of evidence.[42] He warned that both lawyers and judges "increasingly must be vigilant about identifying and knowing precisely what 'evidence' is being admitted."[43] Discussing the importance of electronic documents and particularly the metadata within them, Justice Crothers pointed to both North Dakota's Rules of Professional Conduct as well as the ABA's newly-revised Rule 1.1.[44] Such heightened technology competence for both lawyers and judges is necessary "as the nature of adjudicative evidence shifts from one-dimensional paper to multi-dimensional electronic documents."[45]

E. Technology Incompetence in E-Discovery Is No Excuse (Part I)

In *James v. National Financial, LLC*,[46] the Delaware Court of Chancery was not sympathetic to the defense counsel's explanation for failures to produce requested electronically-stored information – the explanation was that he was "not computer literate."[47] 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.[48] National Financial had been ordered to produce electronically-stored information about each of its loans between September 2010 and September 2013.[49] After multiple deficient discovery responses, and several court orders, the court's patience was at an end, and it sanctioned the defense to deemed admissions and monetary sanctions.[50] 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."[51] Pointing out that "[t]echnological incompetence is not an excuse for discovery misconduct[,]" the court reminded counsel that technology competence was specifically

---

[40] *Id.* at 188.
[41] *Id.* at 188–89.
[42] *Id.* at 193–96 (Crother, J., concurring).
[43] *Id.* at 195.
[44] *Id. See also* MODEL RULES OF PROF'L CONDUCT r. 1.1 cmt. 8 (AM. BAR ASS'N 2012); N.D.R. Prof. Conduct 1.1.
[45] *Ratliff*, 849 N.W.2d at 196.
[46] No. 8931-VCL, 2014 Del. Ch. LEXIS 254 (Del. Ch. Dec. 5, 2014).
[47] *Id.* at *34.
[48] *See generally id.*
[49] *Id.* at *7–9.
[50] *See generally id.* at *21–43.
[51] *Id.* at *35.

included in Rule 1.1 of the Delaware Lawyers' Rules of Professional Conduct.[52] The court further stated that: "'[d]eliberate ignorance of technology is inexcusable . . . . [i]f a lawyer cannot master the technology suitable for that lawyer's practice, the lawyer should either hire tech-savvy lawyers tasked with responsibility to keep current, or hire an outside technology consultant[.]"[53]

F. Technology 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.[54] In his case, Gary sought third-party discovery from Wells Fargo, including e-mails between Steven and the bank.[55] In response to the subpoena, Wells Fargo agreed to conduct a search of certain custodians' e-mail accounts using designated search terms.[56] 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 non-responsive information.[57] 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.[58] Unfortunately, because she did not understand the software's functionality, she produced documents that had not been reviewed by her for confidentiality and privilege.[59] In addition, documents that she had flagged as needing redactions were not redacted before production.[60] 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.[61] The 1.4 gigabytes of Wells Fargo files included customer names, social security numbers, the size

---

[52] *Id.* at *35–36.

[53] *Id.* at *38 (quoting Judith L. Maulte, *Facing 21st Century Realities*, 32 MISS. C. L. REV. 345, 369 (2013)).

[54] Christine Simmons, *Lawyer's 'Inadvertent' E-Discovery Failures Led to Wells Fargo Data Breach*, N.Y. LAW J. (July 27, 2017, 12:00 AM), https://www.law.com/insidecounsel/almID/597a5fed160ba0f315083005/.

[55] *Id.*

[56] *Id.*

[57] *Id.*

[58] *Id.*

[59] *Id.*

[60] *Id.*

[61] Serge F. Kovaleski & 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.

of their investment portfolios, portfolio performance, mortgage details, and other information – much of it about the bank's high net worth investors.[62] One file, for example, was that of a hedge fund billionaire with at least $23 million in holdings with Wells Fargo.[63]

As bad as this was, Turiano found out when her opposing counsel disclosed the information to the *New York Times*.[64] Although opposing counsel has denied that they refused to return the inadvertently produced information, Wells Fargo nonetheless had to obtain court orders in New York and New Jersey to prevent further dissemination of the information.[65] In the meantime, Wells Fargo had to contend with the adverse publicity and data breach notification obligations triggered by such an event.[66] 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 [her] review[,]'" and that she "had not reviewed certain emails containing, or with attachments containing, Confidential Information."[67]

Turiano's mistake highlights the ethical risks as well as malpractice exposure that can accompany errors brought about by technology incompetence.[68] Not only could damages include 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. Turiano's mistake 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.[69] In that opinion, lawyers engaging in e-discovery are directed to either become technologically competent, have other counsel or experts who have such competence, or refrain from handling such matters altogether.[70]

G. Lack of Technology Competence Can Cost You Money (Part I)

Barbara Katsos was a solo practitioner in New York.[71] In 2006, she was retained by an ice cream store franchisee for legal advice on dealing with creditors.[72] It did not go well: the owner filed for bankruptcy, fired Katsos in

---

[62] *Id.*
[63] *Id.*
[64] Simmons, *supra* note 54.
[65] *Id.*
[66] *Id.*
[67] *Id.* Affirmation of Angela A. Turiano, Mill Lane Management, LLC and Gary Sinderbrand v. Wells Fargo Advisors, LLC and Steven Sinderbrand, Index No. 652025/2017, Sup. Ct. of N.Y. (July 24, 2017) (Doc. No. 36).
[68] Simmons, *supra* note 54.
[69] Cal. State Bar, Formal Op. 2015-193 (2015).
[70] *Id.*
[71] *See generally* DiStefano v. Law Offices of Barbara H. Katsos, PC, No. CV-11-2893, 2017 U.S. Dist. LEXIS 72137 (E.D.N.Y. May 10, 2017).
[72] *Id.* at *2–3.

2009, retained another lawyer, and sued her for legal malpractice.[73] During discovery, it was learned that Katsos had gotten rid of her office computers without first taking steps to preserve relevant e-mail and electronic files.[74]

In its sanctions ruling, the court took note of Katsos' lack of knowledge about what types of computers were used in the office, whether they were networked, the firm's aol.com e-mail address and password access, and whether e-mails had been preserved.[75] Katsos was unfamiliar with basic terms like "litigation hold" as well.[76] Not only did the court award attorneys' fees and costs against Katsos because of the spoliation, it also found that she had the "requisite culpable state of mind" – although her negligence did not rise to the level of gross negligence.[77] It also characterized her "as a solo practitioner utterly naive about her obligations to preserve electronic evidence[.]"[78]

H. Lack of Technology Competence Can Cost You Money (Part II)

A sixty-eight-year-old lawyer in Canada, John Paul Dillon, lost his license in 2016 due to his inability to adjust to the technology of modern law practice.[79] Described as a "dinosaur" and as "computer-illiterate" in official proceedings before the Law Society of Upper Canada, the lawyer in question did not use a smart phone, did not access his own e-mail, and according to the spouse to whom he delegated his law office operations, "did not even know how to turn a computer on."[80] Unfortunately, this lack of competence and delegation of authority proved to be his downfall.[81] His wife/office manager misappropriated approximately $390,000 from client trust accounts, and she also intercepted and shredded communications from the Law Society about investigations it had initiated into the misconduct.[82] Noting that the lawyer himself was "not dishonest" but was "a dinosaur," the Law Society allowed him to surrender his law license.[83]

I. Check Your E-mail

Wisconsin attorney Stan Davis claimed that he missed a June 6, 2017, deposition in a high-profile case because the deposition notice wound up in

---

[73] *See generally id.*
[74] *Id.* at *23–26.
[75] *See generally id.*
[76] *Id.* at *39.
[77] *Id.* at *59.
[78] *Id.* *65.
[79] *See generally* Law Soc'y of Upper Canada v. Dillon, [2016] ONLSTH 167.
[80] *Id.* at ¶ 17-20, 102.
[81] *Id.* at ¶ 103-114.
[82] *Id.* at ¶ 58.
[83] *Id.* at ¶ 102-113.

his "junk" folder.[84] Davis represented a former University of Wisconsin wrestling coach, Tim Fader, in a lawsuit against the school.[85] Fader claimed he was fired for reporting a sexual assault to police instead of university officials.[86] Davis maintained that "a series of technological snafus" is to blame, and that dismissal of the entire case is too draconian a remedy to be applied.[87]

J. Have an E-mail Address

In 2013, a South Carolina lawyer's license was suspended because she did not have an e-mail address.[88] Cynthia Collie claimed that she had not had a client in thirty years and was retired, and therefore did not have to comply with the compulsory e-mail rule.[89] Collie persistently refused, faxing repeated filings contesting orders to provide a working e-mail address.[90] After warning the determined Luddite about her "'repetitive frivolous filings,'" the South Carolina Supreme Court finally suspended her license.[91]

K. Technology Incompetence Can Get You Disbarred

James Edward Oliver was a veteran bankruptcy practitioner in Oklahoma for thirty years, with a spotless disciplinary history.[92] 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.[93] Licensed since 1967, Oliver had practiced extensively, and the Oklahoma Supreme Court even acknowledged that "[n]o testimony nor any documents showed an insufficiency in [his] knowledge of substantive bankruptcy law."[94] The problem, it seemed, was "technological proficiency."[95] Specifically, that meant e-filing.[96] After Oliver repeatedly failed 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 thirty days.[97] When he failed to show improvement, Judge Hall suspended

---

[84] Debra Cassens Weiss, *Lawyer says he missed deposition because email notice went to his junk folder*, ABA JOURNAL (July 5, 2017), http://www.abajournal.com/news/article/lawyer_says_he_missed_deposition_because_email_went_to_his_junk_mail_folder.

[85] *Id.*

[86] *Id.*

[87] *Id.*

[88] *In re* Collie, 749 S.E.2d 522, 524–25 (S.C. 2013).

[89] *Id.* at 524. Rule 410 of the South Carolina Bar – amended October 17, 2011 – states that lawyers must provide a mailing address, a telephone number, and an e-mail address as well as continue to update that information if admitted to the bar in South Carolina. *Id.* at 522.

[90] *Id.* at 524.

[91] *Id.* at 523, 525.

[92] State *ex rel.* Okla. Bar Ass'n v. Oliver, 369 P.3d 1074 (Okla. 2016).

[93] *Id.*

[94] *Id.* at 1075.

[95] *Id.*

[96] *Id.* at 1076.

[97] *Id.* at 1075.

him for another sixty days after directing Oliver to "have a lawyer on board" to help him.[98] 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 bankruptcy court, after finding that Oliver had paid another lawyer to "ghost write" his assignments.[99]

When Oliver failed to report this discipline to the Oklahoma Bar, he wound up in front of the Oklahoma Supreme Court.[100] In its March 29, 2016 opinion, the Oklahoma Supreme 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."[101] The dissent, however, took a harsher view, faulting Oliver for his "demonstrated incompetency to practice law before the [b]ankruptcy [c]ourt" and calling for a two year plus one day suspension.[102]

L. When Technology Competence Also Means Being Aware of Cyberscams (Part I)

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 cyber intrusions, 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, it can trigger malpractice liability and disciplinary concerns. And in an era rife with internet scams, this also means lawyers who are not tech savvy when it comes to scams are begging for ethical troubles.

Take, for example, Robert Allen Wright, Jr. In 2013, the Supreme Court of Iowa suspended his license to practice law for at least a year.[103] 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.[104] All he needed, it seemed, was to pay approximately $177,000 in taxes, and the funds in Nigeria would be released.[105] Not only was Wright taken in – hook, line, and sinker – by this "Nigerian prince"

---

[98] *Id.* at 1075-76.
[99] *Id.*
[100] *Id.* at 1074.
[101] *Id.* at 1077.
[102] *Id.* at 1078 (Combs, J., dissenting). In 2008, the Kansas Supreme Court suspended another bankruptcy lawyer for the same thing.
[103] *See generally* Iowa Supreme Court Att'y Disciplinary Bd. v. Wright, 840 N.W.2d 295 (Iowa 2013).
[104] *Id.* at 297.
[105] *Id.* at 297.

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."[106] 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.[107] However, the court nevertheless 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 and suspended his license for a minimum of one year.[108]

In a federal court case in Virginia, another lawyer fell victim to a Nigerian online hack.[109] Plaintiff Amangoua Bile and her lawyer, Uduak Ubom, settled an employment discrimination case against Denny's (represented by LeClair Ryan) in 2015.[110] According to the trial court's findings, Ubom's e-mail account, "ubomlawgroup@yahoo.com," was compromised by hackers, and Ubom was apparently aware of this prior to the settlement.[111] When defense counsel received an e-mail from that account, purporting to be from Ubom, they complied with the instructions to complete a wire transfer of the $63,000 in settlement funds.[112] When Ubom contacted LeClairRyan at a later date inquiring about the settlement monies, he was informed that it had already been paid.[113] LeClairRyan was unable to get the money back, plaintiff refused to dismiss the case, and the defendants refused to pay another $63,000.[114]

The court found that both Ubom and his client were aware that "a malicious third party was targeting this settlement for a fraudulent transfer to an offshore account[.]"[115] The court further found that Ubom and his client both knew that his firm's e-mail account was implicated in that fraudulent activity.[116] The court observed that:

---

[106] *Id.* at 297–98.
[107] *Id.* at 300.
[108] *Id.* at 304.
[109] *See generally* Bile v. RREMC, LLC, No. 3:15cv051, 2016 U.S. Dist. LEXIS 113874, at *1–2 (E.D. Va. Aug. 24, 2016).
[110] *Id.* at *1–2.
[111] *Id.* at *3.
[112] *Id.*
[113] *Id.* at *4.
[114] *Id.*
[115] *Id.* at *11.
[116] *Id.*

> [a]s technology evolves and fraudulent schemes evolve with it, the Court has no compunction in firmly stating a rule that: where an attorney has actual knowledge that a malicious third party is targeting one of his cases with fraudulent intent, the attorney must either alert opposing counsel or must bear the losses to which his failure substantially contributed.[117]

Thus, the court held that by being more technology competent, Ubom could have prevented the loss of the $63,000 and preemptively notified opposing counsel.[118]

M. Technology Incompetence During Discovery "Like Leaving Your File on a Park Bench"

The realities of practice in the Digital Age means use of file-sharing technology, whether doing so with clients or during discovery with adverse parties and their counsel. But, that only heightens the need to use such applications and sites in an ethical and competent manner. Our final cautionary tale is the case of *Harleysville Insurance Co. v. Holding Funeral Home, Inc.*[119]

This was an insurance coverage case in which Harleysville Insurance ("Plaintiff") sought a declaratory judgment that it did not have to pay for a 2014 fire loss at Holding Funeral Home ("Defendants").[120] During the investigation, an investigator uploaded video surveillance footage to the filesharing site Box, Inc., sending a hyperlink to the National Insurance Crime Bureau.[121] The investigator also uploaded the insurance claims file and investigation file to the same Box site, sending the same hyperlink to plaintiff's lawyers.[122] When counsel for defendants sought discovery, an e-mail with the hyperlink was produced to them (complete with a confidentiality notice that the e-mail included privileged and confidential information).[123] Counsel for defendants then used the hyperlink, gaining access to the entire claims file – privileged documents and all.[124]

Plaintiff's counsel only learned that privileged documents were in their opponent's possession when they received a thumb drive of documents from defendants in response to discovery requests of their own.[125] They immediately sought to disqualify defense counsel and belatedly assert

---

[117] *Id.* at *41.
[118] *Id.*
[119] No. 1:15cv00057, 2017 U.S. Dist. LEXIS 18714 (W.D. Va. Feb. 9, 2017).
[120] *Id.* at *2.
[121] *Id.*
[122] *Id.* at *4
[123] *Id.* at *3–4.
[124] *Id.* at *4–5.
[125] *Id.* at *5.

privilege.[126] While the federal judge was not happy with defense counsel's actions (she ruled that defendants' attorneys should have realized the Box filesharing site might contain privileged or protected information), she declined to disqualify them.[127] But the judge reserved her most serious criticism for the plaintiffs, holding that the inadvertent disclosure waived the attorney-client privilege and also waived attorney work product protection as well.[128] Noting that the Box site was not password protected and that information uploaded to the site was available for viewing by anyone, the court ruled that Harleysville Insurance had committed "the cyber world equivalent of leaving its claims file on a bench in the public square and telling its counsel where they could find it."[129] The court found it "hard to imagine an act that would be more contrary to protecting the confidentiality of information than to post that information to the world wide web."[130]

The court reasoned that its decision "foster[ed] the better public policy."[131] Calling for competence in the use of new and evolving technology, the court held that if a party chooses to use a new technology, "it should be responsible for ensuring that its employees and agents understand how the technology works, and, more importantly, whether the technology allows unwanted access by others to its confidential information."[132]

As the *Harleysville* case illustrates, cloud-based filesharing tools can be a double-edged sword. While they offer speed, convenience, and accessibility, the ease of use can result in careless mistakes. Given the importance of protecting confidential client information, lawyers have to be careful to use technological tools in a competent manner. In addition, lawyers should be aware of the technology choices that their clients make, and the risks that these choices might pose. In light of the heavy price paid by allowing their client's investigators to use an unsecure Box.com link to share evidence, the attorneys for Harleysville Insurance are now painfully aware of this.

III. CONCLUSION: INITIATIVES TO IMPROVE TECHNOLOGICAL COMPETENCE

With over half the states and the ABA[133] itself mandating technology competence for lawyers, and with an ever-growing array of cases and disciplinary actions underscoring the risks of *not* maintaining such competence, the need for tech competence is clear. More and more articles

---

[126] *Id.* at *5–6.
[127] *Id.* at *22–23.
[128] *Id.* at *17–18.
[129] *Id.* at *13.
[130] *Id.* at *13–14.
[131] *Id.* at *14.
[132] *Id.*
[133] Simons, *supra* note 4.

(like this one) and CLE presentations are being offered to raise awareness of this issue. But as a practical matter, how do we go about achieving the goal of technological competence?

The key is education. In 2017, Florida became the first state in the country to mandate not only technology competence, but also technology training.[134] Florida beefed up its CLE requirements to require lawyers to complete a minimum of three hours of CLE every three years in approved technology programs.[135] Another educational option comes from the private sector. Former Kia in-house counsel Casey Flaherty and his company Procertas offer a Legal Technology Assessment ("LTA").[136] The LTA assesses lawyers' proficiency with the basic technology tools that are mainstays of modern legal practice, including Word, Excel, and other document creation/document management platforms, and offers training in the tasks where lawyers are deficient.[137]

Law schools are getting into the act as well. Boston's Suffolk University Law School now offers a Legal Innovations and Technology Certificate program, consisting of six online courses designed to teach lawyers how to use technology to perform their services more effectively and efficiently.[138] Each course runs for about 10–12 weeks, consuming 2–5 hours of student time per week, at a cost of about $3,000 per course.[139] Law schools themselves are offering students more tech-focused courses to prepare students for the realities of twenty-first century practice. Law School Innovations Index, produced by Michigan State University College of Law, highlights at least thirty-eight law school programs around the country, measuring how well law schools are equipping their students to deliver legal services in the Digital Age.[140] It examines both the study of legal service delivery and innovations, as well as courses that study law at the intersection of technology.[141]

The "new normal" of requiring lawyers to be technology 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

---

[134] Victor Li, *Florida Requires Lawyers to Include Tech Competence in CLE Courses*, ABA JOURNAL (Feb. 2017), http://www.abajournal.com/magazine/article/technology_training_cle/.

[135] *Id.*

[136] *Id.*

[137] *Id.*

[138] Stephanie Ward, *Online Certificate Program in Legal Innovation Offered by Suffolk Law*, ABA JOURNAL (Oct. 31, 2017), http://www.abajournal.com/news/article/online_certificate_program_in_legal_innovation_offered_by_suffolk_law.

[139] *Id.*

[140] Stephen Rynkiewicz, *Michigan State institute tracks law school innovation*, ABA JOURNAL (Nov. 7, 2017), http://www.abajournal.com/news/article/michigan_state_institute_tracks_law_school_innovation.

[141] *Id.*

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.