Tech Tock, Tech Tock: The Countdown to Your Ethical Demise

by
Stuart Teicher*

I. Introduction

There's a running joke in the continuing legal education industry. No ethics seminar, it goes, is legit unless the lawyers are told not to steal from their trust accounts. It doesn't matter whether the program is about conflicts, confidentiality, or anything else, lawyers hear that admonition at every program. There's a caveat that's emerging to that standard warning. Today we also hear "watch out for the ethical issues with technology."

There's no question that the pace of technology advancement has wreaked havoc in the practice. And the ethical implications are certainly enormous. Lawyers know that. But lawyers continue to struggle with understanding the nuances of those ethical issues. This article will tackle those details, even though the reader is still likely to hear every CLE lecturer address technology in some form.

Oh . . . and don't steal from your trust account.

II. Overlapping Ethics Duties . . . Which Are Broadening

A. *Competence and Technology*

Go ahead, raise the usual complaints. Typically the more seasoned attorneys say things like, *I don't have any desire to get involved in social media . . . I don't want to engage in new technologies . . . I don't need these things in my practice.* On the other hand, newer lawyers often moan, *I don't have the time to keep up with this stuff, I am buried in work . . . I need to bill more hours*

* A lawyer and professional legal educator, who is also an adjunct professor of law at Georgetown Law.

because I have so many loans to pay. Well, there is a simple response to those sentiments:

Tough.

Lawyers are required to understand the latest technology to maintain their minimum level of competence. That mandate is found in the Delaware Rules of Professional Conduct ("Delaware Rules"), and it's also been reinforced in state ethics opinions. For instance, in ABA jurisdictions, Rule 1.1, Competence, states: "A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."[1]

In addition, Comment [8] to Rule 1.1 is explicit about technology: "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." Finally, a variety of state advisory opinions from the last several years have made it clear that lawyers have a duty to understand technology.[2] At this point the obligation to understand basic technology related to the practice of law should be considered common knowledge. But there's one extension of that duty that should be explained—recent opinions have confirmed that a lawyer's duty of competence regarding technology is not static, rather it changes.

A lawyer's duty of competence is broadening. In *The State Bar of California's, Standing Committee on Professional Responsibility and Conduct,* in 2015 the California Bar faced a situation where a lawyer had only a basic knowledge of e-discovery. That surface knowledge ended up getting him in trouble and caused harm to the client (for reasons that we won't go into here). The Bar explained that the lawyer should have had a better understanding of e-discovery. Specifically, it stated that, "An attor-

---

[1] DELAWARE RULES OF PROF'L. CONDUCT R. 1.1. I'd like to reprint the actual text of the ABA Model Rules of Professional Conduct because most states' rules are a derivative of that code. However, copyright restrictions prevent me from doing so. As a result, every time I cite and set forth the text of what I might refer to as the ABA Rule or the ABA "style" rules, I am actually providing the text of the Delaware Rules of Professional Conduct which are the same as the ABA code, but not subject to the same copyright restrictions.

[2] *See, e.g.,* Cheryl B. Preston, *Lawyers' Abuse of Technology*, 103 CORNELL L. REV. 879, 884-88 (2018).

ney's obligations under the ethical duty of competence evolve as new technologies develop and become integrated with the practice of law."[3] The California Bar made it clear that as the technology used in the practice changes, lawyers' duty to understand those technologies keeps pace. But it went further.

The opinion also made it clear that the lawyer needs to understand how the underlying technology works. The California Bar stated, "Attorney competence related to litigation generally requires, among other things, and at a minimum, a basic understanding of, and facility with, issues relating to e-discovery, including the discovery of electronically stored information."[4] It referenced the specific area of technology and required that the lawyer understand the underlying technology. In this case it was e-discovery, but one can see the point about competence the opinion was trying to make. Lawyers need to stay abreast of new technologies that become integrated in the practice of law, and they must also understand how to use those technologies.

But that is not the limit of the expansion of technological competence duties. Several ethics opinions have expanded that duty of competence into the internet. And it is not just about staying aware of the technology used in the internet, but also about understanding the pitfalls.

A variety of opinions have held that lawyers have a duty to understand the dangers of the internet. The Association of the Bar of the City of New York Committee on Professional Ethics issued a formal opinion in April 2015 which dealt with email scams. When discussing that particular type of thievery, the opinion listed a series of troubling indicators that might have raised concern for the lawyers and said that the lawyer should have seen them coming. In reviewing those factors, the committee said, "A lawyer's suspicion should be aroused by any one or more of these common 'red flags' indicating a scam."[5] The committee could not have been more clear in its mandate to lawyers when it stated, "In our view, the duty of competence includes a duty to exercise reasonable diligence in identifying and avoiding

---

[3] State Bar of Cal. Standing Comm. on Prof'l Responsibility and Conduct, Formal Op. 2015-193 (2015).

[4] *Id.*

[5] N.Y. Bar, Formal Op. 2015-3 (2015).

common Internet-based scams, particularly where those scams can harm other existing clients."[6]

Another case in Rhode Island dealt with a similar issue. There a lawyer acted as a "Pay Master," or an escrow agent for a client he found online. The client gave the lawyer money to deposit in his trust account, then had him disburse those funds to others. The lawyer asked Rhode Island disciplinary counsel for an opinion about whether the scheme was permitted, and counsel basically said that it could be, but that the lawyer should be careful because that set-up was likely to be a scam. Of course, it was a scam and the lawyer was disciplined.[7] The Rhode Island Supreme Court found that the lawyer violated the rule on competence. Basically, the court said he should have known better.[8]

Those cases established what I call the "The Duty Not to Be a Bonehead." Some internet scams are so obvious that a competent lawyer should have seen them coming. It is wise to consider the logical extension of that concept. Not only are lawyers duty-bound to be competent about common internet-based scams,[9] but they must also be competent about common technology-related scams and pitfalls in general. That concept is not so difficult to accept. What is difficult, however, is determining which pitfalls are deemed to be "common" or "obvious," and when they acquire that status.

To a certain extent, this question is similar to the earlier issue about when a technology is deemed to have been integrated with the practice of law. At some point the general-lawyering-public will consider certain platforms and their pitfalls to be commonly known. As for when they are both considered to have reached critical mass, well, that is not so clear. Lawyers just have to figure it out. Sometimes that will be easy—a scam that exists for some time gets a lot of press from bar journals and ultimately will become the topic of one of my CLE programs. A lawyer would be educated on the issue then, if they attended my course called "The Cyborgs Are Coming, The Cyborgs Are Coming." But lawyers need to be worried about the "next" scam. And how

---

6 *Id.*

7 In the Matter of Donald F. DeCiccio., No. 2013-275-M.P.

8 *Id.*

9 *See, e.g.,* Jordan K. Carpenter, *The Ethics of Dealing with Internet Scams Targeting Vermont Lawyers*, 41 VT. B.J. 17 (Fall 2015).

is a lawyer to figure out if a technological pitfall that has not been extensively covered by journalists or teachers has nonetheless acquired "common" status? There are two ways.

The first, rather unfortunate way that lawyers will figure scams out is by getting disciplined. There are always some lawyers who find themselves[10] having their conduct evaluated by a disciplinary tribunal and, after the dust has settled, end up hearing the four worst words that any lawyer could hear. "You should have known." When that happens word spreads through the practice, because when a lawyer gets in trouble other lawyers perk up. There is, of course, another way to get the message without having to take one for the proverbial team: Research.

Lawyers should be actively researching technology issues on a consistent basis. In fact, this type of research should be integrated into daily practice. What the cases and ethics rules have shown is that technology has emerged as a core competency. It is, therefore, every lawyer's duty to continually research both the ways that various technology is being used in the practice, and the software, hardware, internet, and other related pitfalls and scams that might be surfacing. That type of research includes reading bar journal articles, legal tech blogs, and following popular legal tech thought leaders on social media.[11] But it also includes staying abreast of technology-related issues in the larger business world. Read newspapers and business journals that do not originate in the legal field.[12] That's a very important aspect of this research because many scams, concerns, and new technology solutions start in the non-law professional world. Consider this practical example that illustrates that point.

It appears that the U.S. intelligence services are worried that certain security cameras could be used by the Chinese government to spy on U.S. targets. The concern is about cameras made

---

10 To all of you Grammar Police Officers out there, I am aware that my pronoun does not match the subject of my sentence. In my writing seminars I explain that . . . well, I don't care. That's my way of presenting a gender neutral pronoun.

11 Here are three places to start. Try following Bob Ambrogi on Twitter: @bobambrogi and read the ethics blog written by the law firm Thompson Hine at https://www.thelawforlawyerstoday.com. You could also sign up for my ethics threat assessments at www.StuartTeicher.com.

12 Try, for instance, the *Harvard Business Review* and the *Wall Street Journal*.

by Hangzhou Hikvision Digital Technology, a company owned in large part by the Chinese government. Their product, called, "Hikvision (pronounced "hike-vision") was nurtured by Beijing to help keep watch on its 1.4 billion citizens, part of a vast expansion of its domestic-surveillance apparatus. In the process, the little-known company has become the world's largest maker of surveillance cameras. It has sold equipment used to track French airports, an Irish port and sites in Brazil and Iran."[13] They were also used by the Memphis police and the U.S. military. Furthermore,

> Consumer models hang in homes and businesses across the country. At one point, the cameras kept watch on the U.S. embassy in Kabul. . .Hikvision's rapid rise, its ties to the Chinese government and a cybersecurity lapse flagged by the Department of Homeland Security have fanned concerns among officials in the U.S. and Italy about the security of Hikvision's devices.[14]

The report also notes that:

> Some security vendors in the U.S. refuse to carry Hikvision cameras or place restrictions on their purchase, concerned they could be used by Beijing to spy on Americans. The General Services Administration, which oversees $66 billion of procurement for the U.S. government, has removed Hikvision from a list of automatically approved suppliers. In May, the Department of Homeland Security issued a cybersecurity warning saying some of Hikvision's cameras contained a loophole making them easily exploitable by hackers. The department assigned its worst security rating to that vulnerability.[15]

Hikvision, of course, denies that it is involved in any sort of inappropriate activity. "Hikvision says its equipment is safe and secure, that it follows the law wherever it does business and that it worked with Homeland Security to patch the flaws the agency cited."[16]

The concern is that "Last year, hackers took control of hundreds of thousands of cameras, including many made by a Chinese rival of Hikvision, to launch a huge "denial of service"

---

13 Dan Strumpf et al., *Surveillance Cameras Made by China Are Hanging All over the U.S.*, WALL ST. J. (Nov. 12, 2017), https://www.wsj.com/articles/surveillance-cameras-made-by-china-are-hanging-all-over-the-u-s-1510513949.

14 *Id.*

15 *Id.*

16 *Id.*

attack that security experts said made sites run by Amazon.com Inc., PayPal Inc. and Twitter Inc. unavailable for hours."[17]

If the U.S. government is worrying about it, you need to be worrying about it. If the government is worried that products like Hikvision can cause security risks, then you need to be concerned as well. The government's secrets are targeted by the bad guys and lawyers' secrets are also targeted by the bad guys. The government is worried that the Chinese will use these technologies to steal secrets from the United States. You need to worry that the Chinese will steal secrets about your clients. Lawyers are targets. That's because the bad guys know that you are the gatekeeper for a lot of your client's valuable information.

You need to consider how these concerns can manifest in your particular practice. Are the security cameras in your office Hikvision products? Are the security cameras installed by your landlord Hikvision products? Did you even know that your landlord has cameras installed in your office? If they are not Hikvison, then what are you using? Who makes those products? The concept of diligence in Rule 1.3 demands that you ask those kinds of questions so you could properly anticipate any potential traps.

Now to the dicey part— what, if anything must you do? I don't know if it's time to stop using Hikvision. What I do know is that now is the time to start asking questions. . .sit down with your IT people, discuss these issues with your cybersecurity consultants. Scrutinize the developers of the software and hardware that is being used in your office, and come to a decision. But just as important as assessing the risk and determining if there is any action to take—document your decisions. Set forth the research you did, memorialize your diligence, make it clear that you gave this careful consideration and that you actually made an informed decision, instead of ignoring the problem.

B. *Supervision*

Could you imagine that two teeny letters could have big implications? Well in a relatively recent batch of amendments, the ABA made a change to two letters in the title of one of the rules

---

17 *Id.*

that address a lawyer's duty to supervise. That's right, just two letters in the *title* – and that change has profound implications.

First a little bit about the rules. There are two code sections that address supervision, Rules 5.1 and 5.3. The former sets forth a lawyer's obligation to supervise associates, and the latter addresses the duty to supervise nonlawyer assistants. Rule 5.3 illustrates how the lawyer's ethical obligations in this regard are broadening.

Rule 5.3 used to be called, "Responsibilities Regarding Nonlawyer Assistants," but now it's called, "Responsibilities Regarding Nonlawyer Assistance." The last two letters in the final word changed: "assistants" is now "assistance." It's a small change, but it's a big deal because it reflects a growing trend in the world of ethics. Lawyers' duty to supervise is getting bigger.

Lawyers are no longer required to simply supervise our assistants—people like secretaries, paralegals, and other individuals who work in our office. Instead, the obligation is now extended to our assistanCE. The change in spelling (and, thus, terminology) is telling lawyers that anyone that they use in assistance are parties that are now considered to be within lawyers' supervisory orbit. By using "assistance," the drafters are expanding the pool to include parties that we'd once call "independent contractors." And that would include certain vendors. That concept is confirmed by the new Comment [3] to Rule 5.3, which reads:

> 1. Nonlawyers outside the firm. — A lawyer may use nonlawyers outside the firm to assist the lawyer in rendering legal services to the client. Examples include the retention of an investigative or paraprofessional service, hiring a document management company to create and maintain a database for complex litigation, sending client documents to a third party for printing or scanning, and using an Internet-based service to store client information. When using such services outside the firm, a lawyer must make reasonable efforts to ensure that the services are provided in a manner that is compatible with the lawyer's professional obligations. The extent of this obligation will depend upon the circumstances, including the education, experience and reputation of the nonlawyer; the nature of the services involved; the terms of any arrangements concerning the protection of client information; and the legal and ethical environments of the jurisdictions in which the services will be performed, particularly with regard to confidentiality. See also Rules 1.1 (competence), 1.2 (allocation of authority), 1.4 (communication with client), 1.6 (confidentiality), 5.4(a) (professional independence of the lawyer), and

> 5.5(a) (unauthorized practice of law). When retaining or directing a nonlawyer outside the firm, a lawyer should communicate directions appropriate under the circumstances to give reasonable assurance that the nonlawyer's conduct is compatible with the professional obligations of the lawyer.[18]

The comment reveals the drafters' motivation for making the change. Basically, it was brought about because lawyers now outsource many of the tasks that were once completed in-house, and there is an increased reliance on technology-related vendors.

One set of vendors in particular, that the comment says are covered by this expansion of the lawyer's duty to supervise, are cloud storage vendors. In fact, several opinions throughout the country have confirmed a lawyer's supervisory responsibilities regarding websites that lawyers use to save client information in the cloud. Take, for example, the Illinois State Bar Professional Conduct Advisory Opinion No. 16-06, which states, "We believe that a lawyer may use cloud-based services. However, because cloud-based services store client data on remote servers outside the lawyer's direct control, the use of such services raises ethics concerns of competence, confidentiality and the proper supervision of non-lawyers."[19]

The opinion reiterates the well-known concept that lawyers must take reasonable efforts to protect client information. The opinion confirms the need to supervise cloud storage vendors when it explains that reasonable efforts include the lawyer insuring that the cloud storage provider reasonably safeguard client information.[20] The opinion refused to provide specific requirements for cloud providers. However, it does state that lawyers must conduct a due diligence investigation when selecting a provider.

> Reasonable inquiries and practices could include:
>
> 1. Reviewing cloud computing industry standards and familiarizing oneself with the appropriate safeguards that should be employed;
>
> 2. Investigating whether the provider has implemented reasonable security precautions to protect client data from inadvertent disclosures, including but not limited to the use of firewalls, password protections, and encryption;

---

18 DELAWARE RULES OF PROF'L. CONDUCT R. 5.3, cmt 3.

19 Ill. Bar, Formal Op. 16-06 at 2 (2016).

20 *Id.* at 3.

> 3. Investigating the provider's reputation and history;
>
> 4. Inquiring as to whether the provider has experienced any breaches of security and if so, investigating those breaches;
>
> 5. Requiring an agreement to reasonably ensure that the provider will abide by the lawyer's duties of confidentiality and will immediately notify the lawyer of any breaches or outside requests for client information;
>
> 6. Requiring that all data is appropriately backed up completely under the lawyer's control so that the lawyer will have a method for retrieval of the data;
>
> 7. Requiring provisions for the reasonable retrieval of information if the agreement is terminated or if the provider goes out of business."[21]

This expanded duty of supervision is not limited to cloud storage vendors. The only reason those particular vendors are mentioned in the commentary and related opinions is because that was the hot new technology at the time the amendments were adopted. But as new technologies become integrated with the practice, the type of vendors that could be captured by Rule 5.3 grows. So think about vendors that provide artificial intelligence services, data analysis, project management, etc.

On a tangentially related point, Illinois Opinion 16-06 also mentioned a concern that most lawyers probably don't think about too often—rogue lawyers in their own firm who might purposefully reveal or leak client information. The opinion does not focus on the issue at all, but it is worth mentioning in the context of supervision.

The lawyer's duty to supervise under Rules 5.1 and 5.3 would likely include the need to ensure that the firm be on the lookout for rogue employees. This is a logical extension of lawyers' existing obligations.[22] It happens to be a very real concern,

---

21 *Id*.

22 *See* Donna Lee Elm & Sean Broderick, *Third-Party Case Services and Confidentiality*, 29 CRIM. JUST. 15, 17–18 (Spring 2014), *citing* State Bar of Nev. Standing Comm. on Ethics & Prof'l Resp., Formal Op. 33, at 3 (2006)("Often, the greatest hazard to confidentiality is not from third parties but from existing employees having unfortunate lapses in judgment or weaknesses in the firm's own electronic security system. The Nevada bar recognized the pragmatics of this irony: The risk, from an ethical consideration, is that a rogue employee of the third party agency, or a 'hacker' who gains access through the third party's server or network, will access and perhaps disclose the information without authorization. In terms of the client's confidence, this is no different in kind or

given what's happening in the world today.[23] For example, according to *Forbes*, in 2017 a firm with offices in Bermuda suffered a loss of 13.4 million files and another firm in Panama had 11.5 million documents leaked.[24] Of course, some people will argue that it's impossible to defend against the most cunning of employees who are bent on stealing information. That may be so. But the extent of supervising lawyers' liability will depend on the circumstances. What is important is to understand that the potential for rogue employees taking client information exists and it should be considered seriously.

C. *Broadening of the Definitions Regarding Communication*

It's not just lawyers' ethical duties that are broadening. There are other parts of the code that indicate an expansion of our professional responsibilities. Consider how some "definitions" are changing. Specifically, a variety of sources confirm that the definition of what constitutes a "statement" or a "communication" that would trigger the rules is expanding. The following case offers an illustration.

In 2016 a Missouri woman was indicted for suspected support of Islamic State. Safina Roe Yassin

> called for the killing of U.S. law enforcement employees and military members by retweeting posts that contained their detailed personal information . . . one of the tweets she retweeted contained the line, Wanted to kill. According to the government, this retweet and other social media postings by Ms. Yassin signaled her active support for ISIS and her intention to communicate threats on their behalf.[25]

One of the central questions raised in the case was "how the law should treat retweets, a feature that allows Twitter users to repost other people's tweets. In a court filing last month, Ms.

---

quality than the risk that a rogue employee of the attorney, or for that matter a burglar, will gain unauthorized access to his confidential paper files.")

[23] See Michael S. Schmidt & Steven Lee Meyers, *Panama Law Firm's Leaked Files Detail Offshore Accounts Tied to World Leaders*, N.Y. TIMES (Apr. 3, 2016).

[24] Niall McCarthy, *The Scale of the Paradise Papers Leak*, FORBES (Nov. 6, 2017), https://www.google.com/amp/s/www.forbes.com/sites/niallmccarthy/2017/11/06/the-scale-of-the-paradise-papers-leak-infographic/amp/.

[25] Nicole Hong, *ISIS Retweet Arrest Raises Free Speech Issues*, WALL ST. J., Aug. 13-14, 2016, at A3.

Yassin's lawyer . . . said his client was 'merely reporting someone else's statements.'"[26]

This is important, because it is likely the first case where a prosecuting agency is trying to affix liability on a person as a result of something they shared on social media. The novel theory of the case is that the prosecution is claiming that by redistributing the content, the retweeter is primarily responsible for the statement as if they said it themselves. This is not the first time people are getting in trouble because of something they are posting on the internet—there are lots of cases where people face liability for making some comment on social media. In fact, there have been several articles that address the issue of retweets and defamation.[27] However, it appears that this is the first criminal matter where the defendant was being charged with being primarily liable for distributing another person's content on social media.

Ultimately, this case may fail. There are substantive criminal law issues, as well as First Amendment concerns. But the substance of this indictment aside, this case is about the expanding definition of a person's "statement" or a "communication."

If a prosecutor in the criminal world is taking this position, then it is only a matter of time before a prosecutor in an ethics context takes the position. It is easy to envision some ethics investigator saying that a lawyer's retweet of someone's statement constitutes that lawyers' statement, or "communication" under the rules. The attorney ethics implications are significant. Consider the following hypothetical:

> You're representing a client in a particularly nasty land use application. The client wants to demolish an historic home and the local land use board is opposed to it. There is a lot of hostility between your client and the land use board because the board wants to save the structure. In an effort to put pressure on the board, your client fabricates the following statement and tweets it one evening, "East Bumble board turned down my application for a demolition permit. I

---

26 *Id.*

27 *See* Adeline A. Allen, *Twibel Retweeted: Twitter Libel and the Single Publication Rule*, 15 J. HIGH TECH. L. 63 (2014); Daxton R. Stewart, *When Retweets Attack: Are Twitter Users Liable for Republishing the Defamatory Tweets of Others?*, 90 JOURNALISM & MASS COMM. Q. 233 (2013).

> don't care—starting construction tomorrow! Firing up the bulldozer!" You retweet that statement.[28]
>
> You know the statement isn't true because you were at the meeting earlier in the day where the board tabled the application without denying it. You also know that your client is overseas and has no intention of actually starting construction. He told you a few hours ago that he was going to take to Twitter just to "rattle the board's cage a little."
>
> However . . . one of the land use board members follows you on Twitter and sees the retweet. He believes that your client might actually take the action described and, to avoid the destruction of a potentially irreplaceable historic structure, he directs the board attorney to immediately file for an injunction against your client, which she does. The board incurs a significant cost.

Could this be a misrepresentation that's actionable under the rule? Consider that Rule 4.1 states (in part), "In the course of representing a client a lawyer shall not knowingly: (a) make a false statement of material fact or law to a third person . . . ."[29] Does this statement qualify?

- Yes, it's false—You know the statement is completely fabricated and that there isn't going to be any construction.
- Yes, it was made to a third person—It wasn't just communicated to a third person, it was communicated to a whole lot of third persons.
- Yes, it was material—the other side relied on that statement when it decided to engage in the considerable expense of filing suit.
- Yes, you "knowingly" disseminated the information—that was your state of mind because you knew what you were doing.

The obvious question is whether you can be said to have made the statement. In a world where a retweet constitutes a

---

[28] Caveat—right now you're thinking, "This is ridiculous . . . . no lawyer would be so stupid to retweet such a blatantly false statement." To that I have two responses. (1) Never underestimate the stupidity of some lawyers. You would be shocked at some of the cases I've seen in my years on the disciplinary committee. (2) Maybe it's a bit of an extreme example, but I wrote it that way to illustrate the point. The issue isn't about the advisability of making the statement, it's about ownership of the communication.

[29] DELAWARE RULES OF PROF'L. CONDUCT R. 4.1(a).

person's statement, then yes, you could be deemed to have made that false statement.

This issue would also arise any time a lawyer might make a "communication" in a self-promotional context as well. Rule 7.2(a) states that "a lawyer may advertise services through . . . electronic communication."[30] What if your partner posts on Facebook a statement saying "I'm ready to accept new clients. Call me now for a free consultation!" If you share that post, then you might be responsible for making the electronic communication. That might not be a problem, unless one day you share something that violates the rules. For example, what if you retweeted your partner's post that said something like, "Call Smith and Smith—we can definitely get you out of criminal charges!" That would likely be an unsubstantiated claim of results that would violate Rules in Section 7 from various states across the country. If you are liable for the statements that you share, then you just violated the code.

The point is that the definition of what constitutes a "statement" or a "communication" is in the process of being redefined. Sharing, retweeting, or otherwise redistributing another person's comment might constitute the sharer's primary statement. Be warned of the implications.

D. *Lawyers' Duty to Periodically Review Their Own Technological Presence*

The idea that lawyers should review their social media presence is common sense. But the ethical mandate to do so has only recently been developed. Several states have come forward with opinions mandating that lawyers check their profiles. For example, the New York County Lawyers Association Professional Ethics Committee opined on March 10, 2015 that, "New York lawyers should periodically monitor and review the content of their LinkedIn profiles for accuracy."[31]

For a while that New York opinion was one of the only voices chiming in on the matter. However, the District of Columbia Bar issued an ethics opinion entitled, "Social Media I: Marketing and Personal Use," where it said:

---

30 DELAWARE RULES OF PROF'L. CONDUCT R. 7.2 (a).

31 N.Y. County, Formal Op. 748 (Mar. 10, 2015).

> An attorney must monitor his or her own social networking websites, verify the accuracy of information posted by others on the site, and correct or remove inaccurate information displayed on their social media page(s). As set forth in comment [1] to Rule 7.1, client reviews that may be contained on social media posts or webpages must be reviewed for compliance with Rule 7.1(a) to ensure that they do not create the "unjustified expectation that similar results can be obtained for others." . . . .
>
> It is suggested that lawyers, particularly those who do not frequently monitor their social media pages, those who may not know everyone in their networks well, or those who wish to have an added layer of protection, utilize these heightened privacy settings. Aside from the potential ethical issues discussed herein, there are many good reasons for a lawyer to want to maintain a higher level of control over what content others may place on a lawyer's social media page(s).[32]

There are a variety of reasons why lawyers should review their social media profiles. Many are obvious, but here are two angles you might not have considered:

1. *The platform may change things, even if you didn't*

These platforms change things like the titles to their text boxes, and stuff like that. So you might have entered your list of skills in a text box that was entitled. "Skills & Expertise," but two weeks later that box might be called "Specialties." You might then run into a problem with making a claim of specialization in violation of Rule 7.4.[33]

2. *Someone else might post something that violates the rule*

It's well established that lawyers can not make statements that create the unjustified expectation that results they obtained for one client can be obtained for others. What if someone else posts such a claim on your site? It's your site and you'd probably be responsible according to the New York County bar opinion discussed above. That's reason enough to check your social media pages every once in a while.

---

32 D.C., Formal Op. 370 at 3.

33 DELAWARE RULES OF PROF'L. CONDUCT R. 7.4.

III. Big Data

A. *Introduction*

Every day there's another article about the dangers posed when companies gather people's data on the internet. Whether it is purchasing habits or location services, revealing such information is causing privacy concerns for the larger public. But there is another side of the issue that's not discussed in major publications—the ethical implications for lawyers.

There are two aspects to the idea of "Big Data" that will be covered in this section. The first is the concept of gathering and analyzing the data. The second is what's commonly referred to as "The Internet of Things (abbreviated as IoT). Competence demands that lawyers understand what these things are, so here are the definitions of both.

Big data is exactly what people would think it is—the collection and analyzation of data. That includes purchase histories, locations, and information about literally everything else. After the data is collected it's analyzed to reveal patterns that can be used in various business, political, and other manners. In many instances the data is used to create predictive models.[34]

The best way to give more depth to the topic is read what the professional techies have to say, so here are some excerpts from online sources:

> Big Data works on the principle that the more you know about anything or any situation, the more reliably you can gain new insights and make predictions about what will happen in the future. By comparing more data points, relationships begin to emerge that were previously hidden, and these relationships enable us to learn and make smarter decisions. . . .This process is automated – today's advanced analytics technology will run millions of these simulations, tweaking all the possible variables until it finds a pattern – or an insight – that helps solve the problem it is working on.
>
> Until relatively recently, data was limited to spreadsheets or databases – and it was all very ordered and neat. Anything that wasn't easily organised into rows and columns was simply too difficult to work with and was ignored. Now though, advances in storage and analytics mean

---

[34] Bernard Marr, *How Is Big Data Used in Practice? 10 Use Cases Everyone Must Read*, BERNARDMARR.COM, https://www.bernardmarr.com/default.asp?contentID=1076 (last visited May 30, 2018).

> that we can capture, store and work with many, many different types of data. . ..
>
> To make sense of all of this messy data, Big Data projects often use cutting-edge analytics involving artificial intelligence and machine learning. By teaching computers to identify what this data represents– through image recognition or natural language processing, for example - they can learn to spot patterns much more quickly and reliably than humans.[35]
>
> Harold H. Hines, Jr. professor of medicine and director of the Center for Outcomes Research and Evaluation at the Yale School of Medicine, likened big data to the microscope—a device that didn't do anything on its own but also enabled a new way of seeing. The microscope was a tool that enabled a process that produced germ theory. Krumholz's view of big data's ultimate potential is similar, "It will create immense opportunities." If we do our part to use big data effectively, Krumholz said, it could launch a "new age of discovery."[36]

"The Internet of Things" is also known as "Frictionless Computing." *Forbes* provided a definition of the Internet of Things:

> Simply put, this is the concept of basically connecting any device with an on and off switch to the Internet (and/or to each other). This includes everything from cellphones, coffee makers, washing machines, headphones, lamps, wearable devices and almost anything else you can think of. This also applies to components of machines, for example a jet engine of an airplane or the drill of an oil rig. As I mentioned, if it has an on and off switch then chances are it can be a part of the IoT. The analyst firm Gartner says that by 2020 there will be over 26 billion connected devices. . . That's a lot of connections (some even estimate this number to be much higher, over 100 billion). The IoT is a giant network of connected "things" (which also includes people). The relationship will be between people-people, people-things, and things-things.[37]

Both of these topics are covered in a section about the general idea of "Big Data" because in many instances, they are linked. Often the information being collected is gathered from one's use of the devices that make up the Internet of Things.

---

35 *Id.*

36 Nicholas A. Christakis et al., *Is Big Data Bigger than Its Own Hype?*, INSIGHTS (July 3, 2017), https://insights.som.yale.edu/insights/is-big-data-bigger-than-its-own-hype.

37 Jacob Morgan, *A Simple Explanation of "the Internet of Things,"* FORBES (May 13, 2014), https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#74d880af1d09.

Big data can be used in the practice of law in a variety of ways. It could be useful in analyzing transactions to determine the probability that a deal will close, or whether a litigant will be successful in litigation. However, the focus of this section is on the ethical issues that lawyers face.

Lawyers hold client information and, to that extent, are data collectors of sorts. But attorneys do not have the same ethical concerns as the data gatherers. For instance, the generic ethical issues that are faced by the collectors of big data encompass issues like whether the data was obtained with consent; does the data consist of sensitive information; was the data gathered in compliance with privacy laws, and; to whom will that data be distributed? While there might be some overlap, lawyers are generally not concerned with those issues. That is because lawyers are not in the business of gathering data from others; rather, lawyers are purposely given data by clients. As a result, the concern for lawyers is very often the exact opposite—keeping the client's data secure. Sharing data is the last thing lawyers want to do.

B. *The Usual Ethical Suspects*

It seems that every technology/attorney ethics issue ends up implicating the same few ethics principles. It should not be a surprise that lawyers are concerned about Competence (Rule 1.1), Diligence (Rule 1.3), Supervision (Rules 5.1 and 5.3), and Confidentiality (Rules 1.6).[38] What differs is the way these ethical issues manifest themselves.

1. *Competence*

After reviewing the various opinions discussed above, it appears a lawyer's duty of competence probably already includes big data.[39] The idea that entities are collecting, sharing, and analyzing data about lawyers and their clients is common knowledge. Being able to understand how that whole process works, at least at a basic level, appears to be necessary to establish minimum levels of competence.

---

38 DELAWARE RULES OF PROF'L. CONDUCT R. 1.1, 1.3, 1.6, 5.1, 5.3.

39 Regarding the generally expanded duty of technology competence, see Jamie J. Baker, *Beyond the Information Age: The Duty of Technology Competence in the Algorithmic Society*, 69 S.C. L. REV. 557, 564 (2018).

2. *Confidentiality*

As a receptacle of client confidential information, lawyers need to be concerned about protecting that information from data collectors. Lawyers have a duty to protect that information and it is set forth in Rule 1.6(c) which states, "A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."[40] The obvious question is, *what is reasonable?* That could change, depending on the type of technology involved. For example, the Wisconsin state bar reviewed the permissibility of using cloud computing in the practice of law. It stated that "cloud computing is permissible as long as the lawyer uses reasonable efforts to adequately address the potential risks associated with it."[41] According to Wisconsin, "To be reasonable, the lawyer's efforts must be commensurate with the risks presented by the technology involved, the type of practice, and the individual needs of a particular client."[42]

Most lawyers probably have no idea about the "particular risks" associated with big data accumulators potentially collecting their client's data from the lawyers themselves because they probably don't understand the particular ways that the data is being collected: Cookies . . . free signals jumping between mobile devices . . . location services . . . and much more.

3. *Advising*

Part of lawyers' duty to advise these days, according to Rule 2.1, includes some duty to explain the pitfalls of technology to clients. Years ago a lawyer would never even think of discussing the negative ramifications of Twitter with a client. However, these days it's almost malpractice if lawyers do not warn corporate clients about saying stupid things on Twitter, lest they go viral and hurt the company. This country is probably at the same point when it comes to big data. Sure, clients know that their whereabouts are being recorded by their phones and that the photos they take contain location identifying information. But do they really appreciate the extent to which they're being

40 DELAWARE RULES OF PROF'L. CONDUCT R. 1.6(c).

41 Wis., Formal Ethics Op. EF-15-01 at 2.

42 *Id.*

tracked? For instance, radio-frequency identification (RFID) tags are being inserted into ski lift tickets to cut back on fraud and wait times at the lifts, as well as help ski resorts understand traffic patterns.[43] All of that tracks patrons' whereabouts in an intrusive manner. Some clients might not realize the extent to which they are being tracked until it hurts them in some way. Then they're going to turn to their lawyer and ask why they weren't warned. Thus, these days, that duty probably includes pointing out the dangers of big data collection and explaining how that could impact their case.

4. *The Convergence*

Here is where the duty of competence, the duty of confidentiality, and the requirement that lawyers properly advise a client converge. If lawyers want to adequately address the potential risks associated with big data, they need to understand the underlying technology and how the collectors are gathering and using that data. Plus, lawyers will need to have that level of understanding to fulfill their duties as an advisor. Furthermore, lawyers will need to be aware about how the technology advances because that is the only way they can maintain competence and ensure that their advice is still relevant. For example, at what point will it be mandatory to have a basic understanding of algorithms? Those formulas are a critical part of big data analyzation. How are they being used to collect clients' data, analyze it, and what, if anything, should lawyers advise clients about it?

As lawyers start to research the ways that big data is being used, they start to see other issues. For example: "Retailers are able to optimise their stock based on predictions generated from social media data, web search trends and weather forecasts."[44] Could this lead to securities fraud? Should in-house counsel or those with a corporate practice be worried/wondering/staying on top of this? It's a big circle of competence, confidentiality, and advising. It's like an ethical dog chasing its tail.

---

43 Marr, *supra* note 34.

44 *Id.*

C. *Putting Pieces Together*

1. *Generally*

One of the biggest concerns with the gathering of big data is the ability of the collectors to put a lawyer's information together. The amount of information they could learn about who clients might be, what lawyers are being retained to do for them, where lawyers keep their confidential information, etc. is worrisome. The entire issue is perfectly illustrated in this one paragraph where an author was touting the power of this technology:

> Say for example you are on your way to a meeting; your car could have access to your calendar and already know the best route to take. If the traffic is heavy your car might send a text to the other party notifying them that you will be late. What if your alarm clock wakes up you at 6 a.m. and then notifies your coffee maker to start brewing coffee for you? What if your office equipment knew when it was running low on supplies and automatically re-ordered more? What if the wearable device you used in the workplace could tell you when and where you were most active and productive and shared that information with other devices that you used while working?[45]

The interconnectedness of people's devices and the notifications that are triggered by and among them are astonishing. A great example of how this could negatively impact lawyers involves the recent merger of LinkedIn and Microsoft.

2. *The Concerns with the LinkedIn/Microsoft Merger*

A short while ago Microsoft bought LinkedIn. A review of the recent news articles announcing the acquisition reveals that a key motivating factor in Microsoft's purchase of LinkedIn was access to LinkedIn's data. Of course, sharing data is nothing new. But when companies improve their ability to share citizens' data across various platforms, lawyers should be on alert. Not just because it is creepy or because of obvious privacy implications. The type of data sharing they're contemplating in the Microsoft/LinkedIn combination raises concerns about confidentiality (and other) issues.

Why are they merging? Microsoft sees a critical synergy with LinkedIn:

> LinkedIn's users are, arguably, Microsoft's core demographic. They also offer Microsoft something it has long sought but never had—a

45 Morgan, *supra* note 37.

> network with which users identify. Microsoft needs to persuade LinkedIn users to adopt that identity, and use it across as many Microsoft products as possible.
>
> Access to those users, as well as the enormous amounts of data they throw off, could yield insights and products within Microsoft that allow it to monetize its investment in LinkedIn in ways that the professional networking site might not be able to. [Microsoft CEO] Mr. Nadella already has mentioned a few of these, including going into a sales meeting armed with the bios of participants, and getting a feed of potential experts from LinkedIn whenever Office notices you're working on a relevant task.[46]

In other words, Microsoft wants to have people's Outlook and other Microsoft software products speak to their LinkedIn profile. The intersection of that data is valuable — various sellers of products and services would be willing to pay for it.

It appears that Microsoft wants to be able to read through the work we do on their products like Word, review our upcoming appointments in our Outlook calendar, search for keywords in our emails, and then find connections with people with our LinkedIn connections. That's what they are searching for – connections they could monetize.

For instance, assume accountant X has an Outlook Calendar appointment which sets a meeting with "Charles McKenna of Account-Soft Corp." Microsoft could then search LinkedIn and it would learn that McKenna works for a company that sells workflow management software. Well, now Microsoft knows the accountant is in the market for workflow management software . . . and it could sell that knowledge to other software companies who would then direct solicitations in the accountant's direction. That's an annoyance for an accountant, but a potential ethics disaster if he or she were a lawyer.

There's a basic issue to be concerned about— confidentiality. If Microsoft scours lawyers' Word documents and emails, then there could be Rule 1.6 confidentiality issues. The more unusual issues come from the calendar function: if the company leverages the data in lawyers' calendars, it could reveal client relationships.

---

46 Christopher Mims, *Why Microsoft Bought LinkedIn*, WALL ST. J. (June 14, 2016), http://www.wsj.com/articles/microsoft-gains-link-to-a-network-1465922927.

The substance of what we learn from the client is confidential, but so is the very existence of the lawyer-client relationship. Will the integration of these platforms make it easier for people to figure out who lawyers represent?

Think about how much information Microsoft could piece together from a single attorney's calendar. It might see a potential client introduction (which lists Pete Smith as present), a court appearance (which lists Pete Smith as present), and a meeting for settlement purposes (which lists Pete Smith as present). It is not going to be too tough for the Microsoft bots to figure out that Pete Smith is the lawyer's client.

If Microsoft can leverage data in a lawyer's calendar, it could reveal key substantive information that could harm the client:

If Microsoft looks at a lawyer's calendar it can see that the lawyer is heading to a particular locale. It might then cross reference the lawyer's LinkedIn connections and send a message to one of them that says something like, "Your connection Bruce Kramer is going to Chicago next week. Why don't you look him up?"

That heads-up might give someone the incentive to look into the lawyer's movements a bit more . . . and who knows what they could find. What if that information was given to a real estate agent that the lawyer knows in Chicago . . . and maybe the lawyer is representing a successful land owner . . . and is clandestinely scouting a real estate purchase. The lawyer would not want people to find this out, because if they figure out that the lawyer is there on behalf of a deep-pocketed client, the purchaser will run up the price. That LinkedIn message that tipped off the real estate agent could cost the client a lot of money.

If Microsoft can leverage data in a lawyer's calendar, it could end up revealing a misrepresentation:

Imagine that Client A asks you to accompany them to a meeting in Los Angeles. You tell her that you can't go because you'll be on vacation on the East Coast. That's not true, however. The truth is that you've already scheduled a meeting with a potentially new client in Los Angeles. You didn't want Client A to know that you'd be in town because you didn't want to have to

shuffle between clients—it would just be too much work. You could have told Client A that you'd be in town but you didn't have time to meet her, but you thought she'd be insulted. It was just easier to say you're far away and be done with it.

Later, Client A gets a LinkedIn message that says, "Your Connection Mary Smith is going to be in Los Angeles next weekend . . . send her a message and try to link up!" Do you know what you are now? Busted. And not only do you have egg on your face, but you may also have committed an ethical violation.

Is the white lie you told your client going to be considered a misrepresentation or deception under Rule 8.4(c)? That rule states: "It is professional misconduct for a lawyer to (c) engage in conduct involving dishonesty, fraud, deceit or misrepresentation . . . ."[47]

You might be thinking . . . it was a white lie. No harm no foul. Well, I searched the ethics code, and I didn't find the term "white lie" or "half-truth" anywhere in the code. You should also note that Rule 8.4(c) does not require that the misrepresentation be "material." That word "material" is simply not in the blackletter rule. Rule 8.4(c) does not allow you to lie about inconsequential things and there is no modifying language—it just says that you can not lie or deceive.

These are just a few issues. Some of these are clear ethics concerns, others are more akin to public relations nightmares. Are they so terrible that lawyers all need to get off LinkedIn right away? It is unclear what dangers will actually be realized, or whether any dangers will be realized at all. What is clear is that part of being a responsible attorney in this technological age is to be diligent in thinking about these issues. As lawyers practice in an ever-changing technological environment, they need to be aware of the potential problems. Lawyers would be wise to keep an eye on the news and stay abreast about the detail regarding the integration of these two platforms. Then, if you determine that you need to act, do so. That way we are "keep[ing] abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology."[48]

---

47 DELAWARE RULES OF PROF'L. CONDUCT R. 8.4(c).

48 DELAWARE RULES OF. PROF'L. CONDUCT R. 1.1, cmt. 8.

D. *The Problem with the IoT*

1. *Frictionless Computing*

The next ethical landmine for lawyers is located in their cell phones. Specifically, lawyers may be very close to the point where they need to have two devices—one for work, and one for personal use.

In recent years, cell phone sales growth has stagnated. After years of incredible growth in sales, the pace of that growth has subsided significantly. The new frontier is in mobile device software. Specifically, the future lies in "frictionless computing."

> Amazon's Echo speaker, which uses Alexa, and Snap Inc.'s new Spectacles, camera-bearing sunglasses, are examples of what Benedict Evans, partner at venture-capital firm Andreessen Horowitz, calls "frictionless computing"—easy-to-use devices that unite applications with hardware beyond smartphones. Ben Schachter, senior analyst at Macquarie Capital, says: "Our view is the next big innovation will be from outside the device—from the software." He expects increasing use of such software to meet entertainment, health-care, home innovation and automotive needs.[49]

The words in that quote that should give lawyers pause are "outside the device." That's because the increased use of cell phones to connect with external hardware by way of an installed app increases the likelihood that hackers can get access to devices. A similar concern surfaced quite recently in the medical community, with the vulnerability of heart devices to hacking:

> On Monday, the U.S. Food and Drug Administration published a public safety notice confirming it is possible for a hacker to remotely compromise security in St. Jude's wireless communication network and then secretly change commands in a pacemaker or implantable defibrillator while it's still wired to a patient's heart . . . ."As medical devices become increasingly interconnected via the internet, hospital networks, other medical devices and smartphones, there is an increased risk of exploitation of cybersecurity vulnerabilities, some of which could affect how a medical device operates," the FDA's Monday safety alert says.[50]

---

49 Betsy Morris, *The Next Big Thing in Smartphones? The Software*, WALL ST. J. (Jan. 11, 2017), http://www.wsj.com/articles/the-next-big-thing-in-smartphones-the-software-1484139602.

50 Joe Carlson, *FDA Says St. Jude Heart Devices Vulnerable to Tracking*, STAR TRIB. (Jan. 10, 2017), http://www.startribune.com/fda-says-st-jude-heart-devices-vulnerable-to-hacking/410153595/.

2. *Hacking*

Although many of these opportunities to exploit devices have existed for a while, the concern is the increased chance of compromising data. As the use of this technology grows, there are increased opportunities for phishing, wireless hacking, etc. Thus, as frictionless computing becomes more prevalent, it greatly increases the opportunity for the hackers to get individuals' private information.

Many lawyers use their personal devices to access work information. They like to have remote access to notes apps like Evernote and cloud storage sites like DropBox. Lawyers text clients and receive work emails, and that is all sent to and from personal devices. It is that same device that will be used to engage further in frictionless computing—many lawyers are probably Alexa addicts already, for instance. To date, lawyers feel comfortable mixing business and personal use because they put password protections on the device and take other reasonable measures to protect client information. But at some point, vulnerabilities will increase to such an extent that the definition of what constitutes "reasonable measures" will change. The increased use of frictionless computing is likely to hasten that change.

Today it might be reasonable to insert a password to restrict access to the phones. But if frictionless computing increases the opportunities for criminals to hack into devices, then it might not suffice to simply have a password or thumbprint barrier to access phones. The prudent move might be to get another device altogether for work matters. Maybe that work device won't be used for frictionless computing at all. Maybe the security measures taken with that work-only device will be more stringent than with personal devices. Then, lawyers can make use of the wonders of frictionless computing, etc., without taking unreasonable risks that compromise client information.

Bear in mind that this isn't about eliminating risk. Risk can never be completely eliminated. The central question is, "when does the risk expand to a point where it's necessary to take some different action?" As usual, there is no way to discern exactly when that line is crossed. But the warning signs have already appeared.

IV. Artificial Intelligence (AI)

A. *Introduction*

The expanding duty of competence requires that lawyers understand AI. Artificial intelligence is best described by going to a common reference book. The *Merriam-Webster* dictionary defines it as: "a branch of computer science dealing with the simulation of intelligent behavior in computers" and "the capability of a machine to imitate intelligent human behavior."

Basically, AI is used to conduct what many people refer to as routine tasks which normally take several people many hours to perform. The unique part about this technology is that it tries to mimic human intelligence as it performs the tasks. It factors in all sorts of variables and it is "able to perform tasks that normally require human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages."[51] In the practice of law AI is already used substantially in complicated e-discovery matters.[52] The systems are able to conduct intricate document review processes which would normally take associates or support staff an enormous number of hours to perform. That's one reason why the tasks, while intensive, are also sometimes referred to as "routine."

B. *Confidentiality*

There are already indications that AI can be used to improve speech recognition programs. In that regard, it can certainly be helpful in better dictation systems. Regarding speech recognition, the ethics issues to be concerned with include:

- Is the speech being recorded?
- Are the recordings being saved?
- If so, who owns them?
- Are the recordings being reviewed for AI improvement? If they are, does that raise confidentiality and privilege waiver concerns?

---

51 https://www.merriam-webster.com/dictionary/artificial%20intelligence.

52 Jason Krause, *Predictive Coding Has Something to Prove Courts and Judges Embrace It, but Is It Really Fixing Discovery?*, 101 ABA J. 32 (Feb. 2015).

Those questions all raise issues of confidentiality under Rule 1.6.[53] If the speech is being recorded and disseminated, then the lawyer could be violating the duty to keep client information confidential. In addition, consider the privilege implications. If some vendor is getting access to information that is covered by privilege, then dissemination of it could amount to a waiver of the privilege (which, most likely, the lawyer had no authority to waive).

C. *Supervision*

The future of AI in the practice will probably mirror the future developing in other business categories. Specifically, AI may be used in "predictive coding."

> Essentially, predictive coding is a process whereby a machine learns from watching human behavior and then applies what it learns. This is the technology behind how Amazon and Google seem to always know what you are looking for before you start looking. The machine's learning algorithms are designed to gather data, analyze it, and then make decisions about what is relevant. And because of the increased computing power on these machines, this is done very quickly.[54]

In other industries predictive coding can help food delivery companies determine how long the food will take to get to consumers. Then they decide which delivery person, route, etc., will be utilized so they get the food to the purchasers as hot as possible. It's also being used to diagnose hypertension, play poker, pass IQ tests, and a range of other novel (and hopefully some useful) things. Many people believe that the legal world will start to use AI in the areas of negotiation and strategy development.[55]

If the machine watches human behavior, then applies what it learns, it could evaluate the probabilities of various outcomes and deliver valuable information that would assist a client in making strategic decisions. While that concept seems to foreshadow the elimination of attorneys, in a strange way it also reveals the reason lawyers will actually never vanish from the

---

53 https://www.merriam-webster.com/dictionary/artificial%20intelligence.

54 Blair Janis, *How Technology Is Changing the Practice of Law*, 31 GP-Solo (May/June 2014), http://www.americanbar.org/publications/gp_solo/2014/may_june/how_technology_changing_practice_law.html.

55 *See, e.g.,* Ayelet Sela, *Can Computers Be Fair? How Automated and Human-Powered Online Dispute Resolution Affect Procedural Justice in Mediation and Arbitration*, 33 OHIO ST. J. ON DISP. RESOL. 91 (2018).

equation. The ability of AI to perform these types of tasks in an efficient manner means that there will very likely be a decrease in the number of support staff that lawyers require. There will also probably be a decrease in the need for the vast number of junior associates, since they perform a lot of the routine tasks that AI will now address. But while there will be a decrease in the number of lawyers that might be needed, there will always be a need for human counsel.

From an ethics point of view this raises interesting issues about supervision. In particular it shows a morphing of the duty. Law firms may be replacing associates with a technology that can do the job they once performed. There are two angles that must be considered.

First, this replacement puts an increased emphasis on supervising . . . our technology people. Although associates may be replaced by software, the software that replaces them does not run itself. Support personnel are always needed to make these things work. And those support personnel might not be located in the lawyer's office—they might be some third party contractor or employees of the company that provides the software. Right now lawyers should be thinking about Rule 5.3.[56] Those support personnel would probably be considered the "nonlawyer assistance" that lawyers are required to supervise according to Rule 5.3. And lawyers should not be fooled into thinking that they don't need to supervise them just because they are an independent consultant. As discussed earlier, the "nonlawyer assistance" category is expanding and a tech vendor who helps run lawyers' AI services is probably going to be covered by Rule 5.3.[57]

Second, and this may be a stretch, but it is not so crazy. . . could a duty emerge to supervise the *technology*?[58] The new Rule 5.3 refers to "nonlawyer assistance." Admittedly, the rule currently refers to the lawyer's need to "make reasonable efforts to ensure that the *person's* conduct is compatible with the profes-

---

56 DELAWARE RULES OF PROF'L. CONDUCT R. 5.3.

57 DELAWARE RULES OF PROF'L CONDUCT R. 5.3 cmt. [3].

58 Katherine Medianik, Note, *Artificially Intelligent Lawyers: Updating the Delaware Rules of Professional Conduct in Accordance with the New Technological Era*, 39 CARDOZO L. REV. 1497 (2018).

sional obligations of the lawyer . . . ."[59] In referring to those nonlawyers, Rule 5.3, Comment [2] states

> Such assistants, whether employees or independent contractors, act for the lawyer in rendition of the lawyer's professional services. A lawyer must give such assistants appropriate instruction and supervision concerning the ethical aspects of their employment, particularly regarding the obligation not to disclose information relating to representation of the client, and should be responsible for their work product. The measures employed in supervising nonlawyers should take account of the fact that they do not have legal training and are not subject to professional discipline.[60]

As these systems get more complex, and as firms start to eliminate staff and allow lawyers to utilize these systems directly, the systems, themselves, could be seen as virtual assistance that requires supervision by the lawyer. This comment could be altered ever so gently to include the systems, in addition to humans.

Alternatively, perhaps the growth of artificial intelligence will mean greater emphasis on supervising the programmers, developers, and the support personnel who create and implement these systems. But the trend of the ethical rules is to expand lawyer responsibility for knowledge of technological systems.

All of that being said, AI is not going to eliminate lawyers all together. Artificial intelligence can never actually substitute for the judgment and advice that a lawyer provides to a client. It could assist in trying to predict outcomes, but the conversation — the consultation — that must occur before a client makes a big decision can not be offloaded to a computer. There are far too many emotional, political, and perhaps public relations considerations that must be taken into account.[61] Wise lawyers will recognize the areas where the practitioner can provide value to a client and focus their efforts (and their marketing plans) in those areas.

As far as the other ethical issues that lawyers will face when *using* AI, the competence, communication, and confidentiality issues are not difficult to grasp. Greater ethics concerns arise regarding the challenges that existing lawyers will face when responding to the changes like artificial intelligence. Not so much

---

59 DELAWARE RULES OF PROF'L CONDUCT R. 5.3(b) (emphasis added).

60 DELAWARE RULES OF PROF'L CONDUCT R. 5.3 cmt. [2].

61 See DELAWARE RULES OF PROF'L CONDUCT R. 2.1, which allows those other factors to be considered in lawyers' legal advice to clients.

the new lawyers—there's nothing for them to "adapt" to, since they're just coming into the practice. I'm worried that a downward pressure on fees and a need to learn about new technology matters will cause veteran lawyers to misbehave more.

If AI causes a reduction in the cost of legal services because of the elimination of some labor needed to conduct certain tasks, then lawyers everywhere will feel that pinch. Even if AI is used by only the largest firms, the reduction in fees will trickle down to small and solo practitioners. Combine that with lawyers who might not have a very congenial mindset toward adopting new technology and it makes for a sticky situation. Existing lawyers who feel these pressures might cut corners more often or resort to unethical conduct in order to make ends meet. In that regard, the veteran lawyers who might fall into that category should remember that the rule on misconduct (Rule 8.4) is broad, and it captures a lot of bad conduct.[62]

D. *Who Calls the Shots?*

The last issue about AI, and it also applies to much of new technology is who gets to decide when lawyers use it? Is the use of technology an objective of the representation, or a means, and why does that matter? For that, Rule 1.2, which discusses the allocation of decision making authority between lawyer and client, may offer some guidance.

Generally, Rule 1.2 says that the client makes decisions about the objectives of the representation and the lawyer gets to decide the means.[63] But the differences between the two are not laid out in the rules (or the comments). On the plus side, there is a bit of direction regarding the criminal context. In those cases the rule explains that lawyers must abide by the client's decision when entering pleas, waiving jury trial, and deciding whether to testify. But there is no direction when it comes to technology.

> Rule 1.2. Scope of representation (in part)
> (a) Subject to paragraphs (c) and (d), a lawyer shall abide by a client's decisions concerning the objectives of representation and, as required by Rule 1.4, shall consult with the client as to the means by which they are to be pursued. A lawyer may take such action on behalf of the client as is impliedly authorized to carry out the representation. A law-

62 DELAWARE RULES OF PROF'L CONDUCT R. 8.4.
63 DELAWARE RULES OF PROF'L CONDUCT R. 1.2.

> yer shall abide by a client's decision whether to settle a matter. In a criminal case, the lawyer shall abide by the client's decision, after consultation with the lawyer, as to a plea to be entered, whether to waive jury trial and whether the client will testify.[64]

So, is technology an objective or a means? It might be both. There's an easy way to get around this, of course. Simply talk to the client. If the lawyer has the appropriate consultation with the client according to Rule 1.4 (as referenced in 1.2(a) above), then the lawyer should be fine.

The future will bring increased pressure on lawyers to stay abreast of technology. It will be necessary to do so in order to avoid disciplinary grievances and malpractice cases. And it won't be important to only understand the law about technology, rather, lawyers will have to understand the underlying technology itself. That explains why states like Florida have already required that lawyers include in their CLE at least three hours of technology education per cycle.[65] Other states will likely follow suit. Thus, it is incumbent on all lawyers to be vigilant in our understanding of new technologies and to constantly reevaluate the ethical implications of using the new platforms that emerge.

---

64 DELAWARE RULES OF PROF'L. CONDUCT R. 1.2.

65 *CLE Requirements FAQ*, FLORIDA BAR, https://www.floridabar.org/member/cle/cler-faq/ (last visited on Nov.19, 2018).