stuartteicher esq
I teach lawyers

Ethics Educator
stuart.teicher@iCloud.com
www.stuartteicher.com
732-522-0371

The Fear Factor—How Good Professionals Get Into Bad Ethical Trouble
Written Materials

HOUR ONE CONFLICTS AND LOYALTY

We all know what conflicts of interest are…basically. Not all of us understand how the rule works nor do we appreciate the fundamental issues about conflicts. That's the place we need to start because you can't understand positional conflicts without first understanding the way conflicts work, generally. Here's the rule in North Dakota:

> RULE 1.7 CONFLICT OF INTEREST: GENERAL RULE
>
> (a) A lawyer shall not represent a client if the lawyer's ability to consider, recommend, or carry out a course of action on behalf of the client will be adversely affected by the lawyer's responsibilities to another client or to a third person, or by the lawyer's own interests.
>
> (b) A lawyer shall not represent a client when the lawyer's own interests are likely to adversely affect the representation.
>
> (c) A lawyer shall not represent a client if the representation of that client might be adversely affected by the lawyer's responsibilities to another client or to a third person, or by the lawyer's own interests, unless:
>
> (1) the lawyer reasonably believes the representation will not be adversely affected; and
> (2) the client consents after consultation. When representation of multiple clients in a single matter is undertaken, the consultation shall include explanation of the implications of the common representation and the advantages and risks involved.
>
> (d) Except as required or permitted by Rule 1.6, a lawyer shall not use information relating to representation of a client to the disadvantage of a client unless a client who would be disadvantaged consents after consultation.

There's an important conceptual issue to understand here. There are always two fundamental concerns that are at the heart of every conflict situation: it's always about either loyalty or confidential information. Every time, in every situation, it's always about one or both of those concepts. Are you being forced to compromise your loyalty to your client because of your loyalty to another person, or do you have confidential information about a client that you are going to use to their detriment.

The North Dakota rule clearly addresses the two major issues in conflicts. In subsection (a), the rule talks about whether a lawyer is "adversely affected." That entire section is all about loyalty. If you are adversely affected, then your loyalty to one client is being compromised by your responsibilities to someone else.

Something I like, particularly about the North Dakota rule, is (b). This section talks about the instance where a lawyers own interests will conflict with that of the client. Every state addresses that in their rule, but few others do so as directly as North Dakota.

The final thing I want to point out is the last section of ND's rule, 1.7(d). Here we see the reference to *using* confidential information. In the usual rule on confidentiality we are concerned about revealing confidentiality. But as you see in ND's rule, the drafters remind us that when it comes to conflicts, there is a concern with using that information. There's a difference — you can use a client's information to their detriment without revealing it. In the former instance, you'd be breaching your duty of loyalty to the client. That's why it's forbidden by Rule 1.7.

<u>Imputing conflicts: The basics: if there's a conflict caused by 1.7 or 1.9, it's imputed per 1.10[1]</u>

Let's say that a lawyer is infected with a conflict. Yes, it's a little unseemly to use that word. I could use "affected," I guess, but I don't want to…and I'm the teacher. So I'm going to

[1] We discuss the quirk for government lawyers (Rule 1.11) below.

call the lawyer who has the conflict *infected*. The other lawyers in the firm— those who are not infected— I'll refer to them as the "other," or "remaining" lawyers. Back to our story….

There's a lawyer who is infected with a conflict. Let's say that a lawyers is a card carrying member of the NRA. She is a certified instructor and has have devoted much of her life to the safe, legal use of firearms. In addition, she is a board member of the NRA and spends a lot of time fighting against what she believes is unreasonable legislation about gun ownership— legislation which she believes does not promote safety, rather, makes society more vulnerable to gun violence. But that lawyer is approached by a client who wants to retain the lawyer to write gun control legislation. The client wants the lawyer to draft the law, advise on its legality, and otherwise assist in the lobbying efforts to get the law passed. However, after reviewing the proposed law that the client wants to enact, the lawyer believes that it's (a) not necessary, and (b) she feels it will actually make gun violence worse, rather than better. Well, under those facts, there's a problem because the lawyer has a conflict.

The conflict is with the lawyer's own personal interests and that runs afoul of Rule 1.7. Rule 1.7 is what one might call the "main" rule on conflicts and subsection (a)(2) says, in part, that a lawyer has a conflict of interest if, "there is a significant risk that the representation of one or more clients will be materially limited by the lawyer's responsibilities to another client, a former client or a third person or by a personal interest of the lawyer." Well, here, we have a situation where there is a conflict with the "personal interest of the lawyer." The lawyer in our hypo will likely have a difficult time lobbying for a bill that will enact the type of legislation that she actively opposes in her daily life.

Incidentally, you might be thinking, "Hey, Teicher, I've seen/heard/attended your other program on conflicts of interest, and I recall that a lawyer could potentially take a client notwithstanding the existence of a conflict in Rule 1.7(a). As long as they get over the hurdles set forth in 1.7(b), they might still be able to take the client." Well, my smart and observant

student, you are right. But in this fact pattern the lawyer probably can't get over the hurdles in 17(b). That's because Rule 1.7(b)(1) requires that the lawyer must reasonably believe that she can provide competent and diligent representation to the client. But given the lawyer's personal beliefs combined with the work that they actively oppose such legislation elsewhere in their lives, it's not likely that they lawyer will be able to provide that competent representation to the client in this case.[2] To borrow the language from Rule 1.7, Comment [8], it's likely that there would be a significant risk that our lawyer's ability to consider, recommend or carry out the appropriate course of action for the client will be materially limited as a result of her other, personal interests.

A word about the intersection of conflicts and confidentiality, using the OJ case

Early in the trial, OJ was supposed to turn himself in. Instead, he went on his infamous run. The prosecution was obviously furious, but so too were OJ's lawyers. OJ's primary defense counsel at the time, Robert Shapiro, made representations to the police that he would accompany OJ to police headquarters and that OJ would voluntarily turn himself in. So when OJ took off, unbeknownst to his own team, everyone was really upset.

When OJ went missing the prosecutor held a press conference where he admonished people who might be assisting OJ. Just after the prosecutor's press conference, OJ's lawyers had a press conference of their own. Author Jeffery Toobin write about it in his book The Run of His Life. Toobin explained that, "Shapiro, too, started with a plea to the camera. But he was aiming for an audience of one. 'For the sake of your children,' he told O.J., 'please surrender

[2] I know what you're thinking— having different beliefs from a client is not necessarily a bar to representation. Agreed. That's why I tried to create a scenario where the lawyer with the conflict doesn't just have different beliefs, but also actually takes action that is contrary to the interest to the client. That, I think, puts them into conflict territory.

immediately. Surrender to any law enforcement official at any police station, but please do it immediately.'"[3]

Of course, as soon as I read that I thought — what about confidentiality???!! Of course, the answer is not so clear. If that were all the lawyer said, then maybe 1.6 wouldn't be invoked — maybe it would not be an issue because no information "related to the representation" was really revealed. If it's just a plea to come back, maybe the lawyer would be ok. On the other hand, what about the fact that the statement reveals that the client is on the run? Does it matter that it's on the news and that the information is publicly available? We will talk about that during the program but the spoiler is…no, it doesn't matter. The commentary to Rule 1.6 says that you need to keep quiet about information relating to the representation, "whatever it's source."

But it doesn't matter because, astonishingly, that wasn't all Shapiro said. He said much more, including:

> "Shapiro began by summarizing the day's events: the early morning call from the detectives, his journey to Kardashian's home, his passing the news of the arrest warrant to Simpson, and the defendant's sudden disappearance. 'I have on numerous occasions in the past twenty-five years made similar arrangements with the Los Angeles Police Department and the district attorney's office and Mr. Garcetti. All of them have always kept their word to me, and I have always kept my word to them. In fact, I arranged the surrender of Erik Menendez from Israel on a similar basis. We are all shocked by this sudden turn of events.'
>
> It was an extraordinary tale, and the reporters, along with the national television audience, listened with rapt attention. Shapiro's account was also highly incriminating of his client. Simpson's actions, as described by Shapiro, did not seem to be those of an innocent man."[4]

Now we need to see if this was okay per 1.6. In order to do that we need to explain how the rule regarding confidentiality is built.

---

[3] Jeffrey Toobin. "The Run of His Life." Apple Books. https://books.apple.com/us/book/the-run-of-his-life/id622206034, Page 217-218

[4] Jeffrey Toobin. "The Run of His Life." Apple Books. https://books.apple.com/us/book/the-run-of-his-life/id622206034, page 218-219

Rule 1.6. Confidentiality of information (in part)
(a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation, or the disclosure is permitted by paragraph (b).
(b) A lawyer may reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary:
(1) to prevent reasonably certain death or substantial bodily harm;

Subsection (a) sets forth the general rule on confidentiality. When I teach this rule to my students I explain that the rule is broken down into "two permissions and the exceptions." Those labels are my words, not the text from the rule. Per the rule, a lawyer can't reveal information related to the representation unless they have:

- Express permission (called, "informed consent" in the Rule)
- Implied permission ("impliedly authorized"), or
- The revelation falls into one of the rule's exceptions ("disclosure is permitted by paragraph (b)).

When it comes to the first "permission," remember that in order to be granted that express permission, you must show that the client gave you "informed consent." Rule 1.6(a). That phrase is an important term of art, so you need to make a point of reviewing two key sources to properly obtain informed consent— specifically, Comment [2] to Rule 1.6 discusses the term, as does Rule 1.0(e). The latter rule is the "Terminology" section of the code, and the term "informed consent" is specifically defined there.

In order to get what I call "implied permission," you need to show that, "the disclosure is impliedly authorized in order to carry out the representation." Rule 1.6(a). It's important to understand that this is not an "exception" to the prohibition against revealing client information. Rather, these instances are times when a lawyer would have been granted permission to do so by virtue of some implied authorization. That could arise in the context of negotiation, or some other scenario when you have some communication or discussion with a client that results in the lawyer being granted implied permission. That implied permission, however, is not an exception to the rule and it's different from the exceptions in paragraph (b).

We all know that there are exceptions to the general rule and those exceptions are set forth in subparagraph (b). That section sets forth those times when lawyers are permitted to

reveal client information, and depending upon the jurisdiction, maybe even required to do so. The problem is that it's hard to keep track of those exceptions. Luckily, I've figured out that there is one word that will guide you.

Catastrophe.

When you look at the different exceptions in Rule 1.6(b), you see that every one of them involves some catastrophe. Actually, the truth is that there are probably *two* words that would accurately describe the times when a lawyer is permitted to reveal information— to avoid catastrophe and to protect our own self-interest. Of course, if our self-interest is compromised it could amount to a personal catastrophe of sorts, so maybe that one word would be enough. Let's look at the rule and the commentary to see what I mean.

So back to the OJ lawyers and their statements to the press. Here are the points we'll talk about during the program:

- Shapiro could not have received informed consent— he didn't know OJ would be running
- It would be tough to argue that the statements were impliedly authorized?
- Maybe he could say that there was a 1.6(b)(1) excretion if he thought he was going to kill himself? That might have worked.

HOUR TWO — BEING AN ADVISOR

When your client won't listen to you — conflicts between you and the client

Who makes the decisions during the representation, lawyer or client? If I asked you to craft an answer, you could probably come up with a phrase that made sense, but I bet it would be relatively vague. That's because it's an easy answer in theory, but it gets tough to apply in real life. The rule that gives us direct guidance is Rule 1.2, which reads as follows:

> 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 lawyer 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.

Can you see how this is setting up a conflict between the lawyer and client? Maybe it's not the type of conflict that would invoke the formal rules regarding Conflict of Interest, but it could create an issue where the opinions of the lawyer and client conflict. So how do we resolve such a situation? The commentary tries (but does not succeed) in giving us some direction:

> Rule 1.2, Comment [2]:
> On occasion, however, a lawyer and a client may disagree about the means to be used to accomplish the client's objectives. Clients normally defer to the special knowledge and skill of their lawyer with respect to the means to be used to accomplish their objectives, particularly with respect to technical, legal and tactical matters. Conversely, lawyers usually defer to the client regarding such questions as the expense to be incurred and concern for third persons who might be adversely affected. Because of the varied nature of the matters about which a lawyer and client might disagree and because the actions in question may implicate the interests of a tribunal or other persons, this Rule does not prescribe how such disagreements are to be resolved. Other law, however, may be applicable and should be consulted by the lawyer. The lawyer should also consult with the client and seek a mutually acceptable resolution of the disagreement. If such efforts are unavailing and the lawyer has a fundamental disagreement with the client, the lawyer may withdraw from the representation. See Rule 1.16(b)(4). Conversely, the client may resolve the disagreement by discharging the lawyer. See Rule 1.16(a)(3).

A review of the rule reveals that the client decides the objectives and we control the means, after consultations (that's where the rule on communication, Rule 1.4, comes in). While that's an easy theoretical concept, it's hard to determine how it translates into practice. What exactly constitutes an objective, versus means? Monumental decisions are easy to put in the former category and trivial matters into the latter. But what about the multitude of issues that fall in between? Unfortunately there isn't any guidance in the rules or commentary and, as usual, we are left to our own devices to figure it all out. Note, however, that there are a few items that are clearly within the client's purview. Those particular instances are set forth in 1.2(a), and make special notice of the difference between a civil and criminal context.

The separation of powers between lawyer and client can't always be resolved and when these conflict, sometimes withdrawal may be required. In those cases we turn to Rule 1.16 for guidance.

The key sections to review are Rule 1.16(a) and (b). These sections talk about situations when withdrawal is either mandatory or permissive. Subsection (a) talks about those situations where withdrawal is mandatory and there's on particular section that is worth pointing out: those instances when a lawyer's physical or mental condition materially impair the lawyer's ability to represent the client. If any of you have taken my courses before, then you know that I'm a big proponent of addressing the "whole" lawyer and that means considering the mental, emotional, and physical implications of the practice. Many of us aren't aware that there are rules that address those situation and here you go.

> Rule 1.16. Declining or terminating representation (in part)
> (a) Except as stated in paragraph (c), a lawyer shall not represent a client or, where representation has commenced, shall withdraw from the representation of a client if:
>
> > (1) the representation will result in violation of the rules of professional conduct or other law;
> > (2) the lawyer's physical or mental condition materially impairs the lawyer's ability to represent the client; or
> > (3) the lawyer is discharged.

(b) Except as stated in paragraph (c), a lawyer may withdraw from representing a client if:

(1) withdrawal can be accomplished without material adverse effect on the interests of the client;
(2) the client persists in a course of action involving the lawyer's services that the lawyer reasonably believes is criminal or fraudulent;
(3) the client has used the lawyer's service to perpetrate a crime or fraud;
(4) a client insists upon taking action that the lawyer considers repugnant or with which the lawyer has a fundamental disagreement;
(5) the client fails substantially to fulfill an obligation to the lawyer regarding the lawyer's services and has been given reasonable warning that the lawyer will withdraw unless the obligation is fulfilled;
(6) the representation will result in an unreasonable financial burden on the lawyer or has been rendered unreasonably difficult by the client; or
(7) other good cause for withdrawal exists.

What Alaska teaches about advising

During the program I'm going to tell you a story about Alaska and relate it to the duty to advise. Here, I'd like to incorporate the history of Alaska and use it to explain Rule 2.1.

If you were to walk to the end of the Kenai Peninsula, hop on a boat and row out to Katmai National Park and Preserve, then walk through the Aniakchak National Monument and Preserve, you'd eventually emerge onto a treeless tundra called the Aleutian Islands.[5] The Aleutian Islands protrude out from the mainland toward the Pacific Ocean and they're named after the indigenous peoples called the Aleuts. "Between ten thousand and forty thousand years ago, the ancestors of Aleuts migrating from Asia to North America settled on these remote islands."[6] What I found most interesting to learn about Aleut culture were the rules that governed their society before they experienced European contact.

Consider, for instance, their approach to business dealing. "Within the village, Aleuts placed the highest emphasis on cohesion, harmony, cooperation, generosity, and avoidance of conflict."[7] That is best illustrated in the manner in which they traded amongst themselves. "Aleuts conducted trade through a third party, called a *tayanak*, who kept secret the identify of

---

[5] Madden, Ryan, On the Road Histories— Alaska, Interlink Books (2005), at page 16.

[6] On the Road at 16.

[7] On the Road at 18.

participants precisely to minimize the possibility of hard feelings."[8] Thus, in an effort to avoid the type of conflict that could create negative tension in the community, the Aleuts developed a system that would minimize that possibility. Instead of relying on system that could create confrontation, they were partial to an arrangement that relied on a neutral third party.

Is it possible that the cultural preference for conflict avoidance survived through the years and embedded itself in modern Alaskan culture? The current ethics rules seem to say yes. To see what I mean, take a look at Rule 2.1 which sets forth a lawyer's duty to advise. The current ABA-style version of Rule 2.1 states:

> In representing a client, a lawyer shall exercise independent professional judgment and render candid advice. In rendering advice, a lawyer may refer not only to law but to other considerations, such as moral, economic, social and political factors, that may be relevant to the client's situation.

There's a good reason for including all of those other factors in the rule. It's because myopically advising a client on legal matters could be inadequate. If you go down to the commentary, you'll see a bit of an elaboration on that idea. Comment [2] to Rule 2.1 explains that "advice couched in narrowly legal terms may be of little value to a client," and that, "purely technical legal advice…can sometimes be inadequate."

A perfect example of that comes from the world of technology and social media. And remember, our fundamental ethics duties evolve as changes occur to the practice. So, for instance in these days where social media is prevalent, our clients need to remember that the things they say can be heard everywhere. We may think you're off the grid, or that no one is listening to you.. but we're not. Ever. We are all just one stupid tweet away from being a meme. And not only will not only be heard everywhere, but those tweets will be amplified. The power of Twitter means that everything you say can be shared and the number of people you reach can be multiplied exponentially. And there is a principle to which I hold fast— the more repulsive your tweet, the more likely that it will be retweeted into oblivion. And the more likely it is that people will become enraged by it. And that can hurt a client. That's why I think our duty to advise has evolved to include the element of "public outrage." We need to warn our clients

[8] On the Road at 18.

about the dangers of public outrage and how it could affect their matter. And that's what the commentary meant when they said that purely technical legal advice could be inadequate.

So the ABA rule on advising is relatively short. just to reiterate, it states:

> In representing a client, a lawyer shall exercise independent professional judgment and render candid advice. In rendering advice, a lawyer may refer not only to law but to other considerations, such as moral, economic, social and political factors, that may be relevant to the client's situation.

And that's it. The Model Rules end there, and your local rule likely reads exactly like that. But in Alaska, there's an additional clause. Not only may a lawyer refer to moral, economic, social and political factors in Alaska, but lawyers here are also permitted to discuss "the availability of alternative forms of dispute resolution, that may be relevant to the client's situation." Alaska Rule 2.1. The comment explains that in a matter involving or expected to involve litigation, a lawyer should advise the client of alternative forms of dispute resolution which might reasonably be pursed to attempt to resolve the legal dispute or to reach the legal objective sought.

I think that the inclusion of this sentence is a direct outgrowth of the local culture I referred to above. The Aleut people created a system that avoided conflict. They used a middleman to conduct business transactions because they were concerned that direct contact among people with competing interests could cause some bad blood. That is, at its heart, a form of alternate dispute resolution. And that is exactly the type of cultural characteristic that is ingrained in a people and finds its way into successive generations. And that's why I think Alaska included that extra line in it's version of Rule 2.1. The history of the people in the region have culturally embraced the value of alternate dispute resolution.

Now, we all know that the idea that one should consider ADR in our advising isn't exclusive to Alaska. The ABA-style code contains something about it in the commentary. Rule 2.1, Comment [5] explains that, "…when a matter is likely to involve litigation, it may be necessary under Rule 1.4 to inform the client of forms of dispute resolution that might constitute reasonable alternatives to litigation." But the placement of that text is instructive. In

the Model Code (and likely in your local code) the language is in the commentary. But the fact that Alaska put it into the black letter text of the rule shows the particular emphasis they want to have on the topic. And it's likely that they made that change because of the local culture that's evolved.

The boundaries of advice — the rules on misrepresentation

There are five rules that deal with the prohibition against making misrepresentations in the law. I call them the "Fab Five of Attorney Lies." But might it be better to call them the Fab Four, Plus One? Read on and let me know what you think…

Rule 3.3. Candor toward the tribunal

(a) A lawyer shall not knowingly:
(1) make a false statement of fact or law to a tribunal or fail to correct a false statement of material fact or law previously made to the tribunal by the lawyer;
(2) fail to disclose to the tribunal legal authority in the controlling jurisdiction known to the lawyer to be directly adverse to the position of the client and not disclosed by opposing counsel; or
(3) offer evidence that the lawyer knows to be false. If a lawyer, the lawyer's client, or a witness called by the lawyer, has offered material evidence and the lawyer comes to know of its falsity, the lawyer shall take reasonable remedial measures, including, if necessary, disclosure to the tribunal. A lawyer may refuse to offer evidence, other than the testimony of a defendant in a criminal matter, that the lawyer reasonably believes is false.
(b) A lawyer who represents a client in an adjudicative proceeding and who knows that a person intends to engage, is engaging or has engaged in criminal or fraudulent conduct related to the proceeding shall take reasonable remedial measures, including, if necessary, disclosure to the tribunal.
(c) The duties stated in paragraph (a) and (b) continue to the conclusion of the proceeding, and apply even if compliance requires disclosure of information otherwise protected by Rule 1.6.
(d) In an ex parte proceeding, a lawyer shall inform the tribunal of all material facts known to the lawyer which will enable the tribunal to make an informed decision, whether or not the facts are adverse.

Rule 3.3 is the most complicated rule in the representation genre. It only seems logical, given the forum to which it applies. We need to be sure that our statements to tribunals are as far away from deception as possible. Not only do we want to avoid deception, but we may need to remediate situations where untrue testimony is provided to a tribunal. In that regard, this rule contains significant guidance regarding our duty to remediate false statements. Note something

else in that regard: this is one of the rules where you should check to commentary. The commentary contains a lot of direction regarding how we remediate and the steps we must take when counseling a client who may have given false testimony to a tribunal. Furthermore, the commentary expands on the differing obligations in a civil and criminal context. More on this rule below.

Rule 4.1. Truthfulness in statements to others

> 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; or
> (b) fail to disclose a material fact when disclosure is necessary to avoid assisting a criminal or fraudulent act by a client, unless disclosure is prohibited by Rule 1.6.

What I find interesting about Rule 4.1 is the limited responsibility with respect to the failure to disclose. Of all the rules addressing misrepresentation, this rule appears to impose the minimum responsibility because it only prohibits the failure to disclose when it's necessary to avoid assisting in a crime or fraud. That's a pretty limited situation. I think it has something to do with the audience.

4.1 governs those situations where we are speaking on behalf of a client, but not necessarily to a tribunal or other authority (since those venues are governed by Rule 3.3). Thus, the rule is most likely in play when we are talking to an adversary. It makes sense that, given the adversarial nature to our system, we would have a limited obligation to disclose when it comes to the opposing lawyer.

Rule 8.1. Bar admission and disciplinary matters

> An applicant for admission to the bar, or a lawyer in connection with a bar admission application or in connection with a disciplinary matter, shall not:
> (a) knowingly make a false statement of material fact;
> (b) fail to disclose a fact necessary to correct a misapprehension known by the person to have arisen in the matter, or knowingly fail to respond to a lawful demand for information from an admission or disciplinary authority, except that this rule does not require disclosure of information otherwise protected by Rule 1.6.

Rule 8.1 deals with several specific instances of misrepresentation. Interestingly, this is the only rule that applies to lawyers before they become members of the bar. But it’s not only applicable to almost-lawyers. In addition to bar applications, in some jurisdictions we also need to be concerned about (this might surprise you) statements we make about CLEs. If you are in a

self-reporting jurisdiction you are likely to see a reference to misleading statement in a CLE context. But there's another item that I this is more important to note and that pertains to disciplinary tribunals.

We can see from the text of the rule that it's improper to make a misrepresentation in connection with a disciplinary matter. But also note this related item: In many jurisdictions, failure to respond to a disciplinary tribunal is grounds for an independent grievance. In many cases it won't matter if you're ultimately exonerated for the underlying charge that got you into ethical trouble—if you fail to respond, you will still face a grievance.

Misrepresentations that may occur when we talk about ourselves or our services are covered by Rule 7.1. That rule is placed in the sections that deal with advertising, so it's common for lawyers to think that 7.1 is only invoked in cases of advertising. Personally, I think it's easier to think of it as being invoked in cases of "self-promotion." Every time you think you're acting in a self-promoting nature, Rule 7.1 could be in play.

Rule 7.1. Communications concerning a lawyer's services

> A lawyer shall not make a false or misleading communication about the lawyer or the lawyer's services. A communication is false or misleading if it contains a material misrepresentation of fact or law, or omits a fact necessary to make the statement considered as a whole not materially misleading.

The reason I say that there are only four rules that address misrepresentation (3.3, 4.1, 7.1 and 8.1) is because the fifth rule, 8.4 Misconduct, is about much more than just misrepresentation. It covers the deceptive type of conduct that we see in this last part of the Pinocchio story. In fact, it almost seems as if misrepresentation in 8.4(c) is an afterthought—or at the very least buried among some other important concepts. Here is the rule, along with some important things to consider in Rule 8.4.

Rule 8.4. Misconduct

> It is professional misconduct for a lawyer to:
> (a) violate or attempt to violate the Rules of Professional Conduct, knowingly assist or induce another to do so or do so through the acts of another;
> (b) commit a criminal act that reflects adversely on the lawyer's honesty, trustworthiness or fitness as a lawyer in other respects;
> (c) engage in conduct involving dishonesty, fraud, deceit or misrepresentation;
> (d) engage in conduct that is prejudicial to the administration of justice;

(e) state or imply an ability to influence improperly a government agency or official or to achieve results by means that violate the Rules of Professional Conduct or other law; or (f) knowingly assist a judge or judicial officer in conduct that is a violation of applicable rules of judicial conduct or other law.

The sections that I find most interesting are (b), (c) and (d). In subsection (b) the rules tell us that misconduct can be the commission of certain crimes that impact our fitness to be an attorney. Do you think that driving drunk would fall in there? Maybe that's debatable. How about drug offenses? Of course it seems to get a little easier when you talk about check fraud or theft. What's interesting, though is that the rule doesn't say that you must be “convicted” of a criminal act, only that you “commit” the act. As a result, discipline may be forthcoming if the criminal behavior occurred, even if there were no formal consequences in the justice system.

Subsections (c) and (d) are what I call the “catch all” sections. For instance, I think we could spend an entire day giving examples of, “conduct involving dishonesty, fraud, deceit or misrepresentation.” What's critical to remember is that the conduct we're talking about is not limited to the things you do in your office-- the rule doesn't make that distinction. That's one of the reasons that I tell attorneys that there is almost no separation between the professional and private life of an attorney. What you do outside the office matters and if your behavior outside the office violates Rule 8.4, you're going to be subject to discipline

Likewise, I could imagine a slew of actions that could be considered “prejudicial to the administration of justice.” What about blogging about how you believe a judge is a thief and a liar? How about stealing evidence out of a courthouse. The list could go on. An interesting side note: 8.4(d) would probably be the section that would be cited in a claims of discrimination in the profession. Many states have adopted specific ethics rules outlawing discrimination, but not all of them. 8.4(d) would serve the purpose for states without a specific prohibition.

Leadership and Communication

You can't please all of the people all of the time. But you can displease most of the people most of the time. It's so easy to make people angry. Trust me, I teach CLE, which means that my very *existence* makes people angry. Think about it — if a lawyer commits minor unethical conduct their disciplinary board might offer them "diversion" where you admit that minor unethical conduct and get the disciplinary version of a slap on the wrist Sometimes that's additional CLE course. That's me. I teach those CLE courses. So think about that…*You didn't communicate with your client? I sentence you to 3 hours of Stuart Teicher.* I am a punishment. It's really not good for my ego.

It's super easy for lawyers to make their clients angry as well. All you have to do is make them call your office twice for the same thing. It's two strikes, you're out. Yes, there is also the issue of an ethics grievance, but even if the disciplinary system doesn't get involved, the client is often mad. And it could also end up leading to an ethics violation. Here is the rule:

> Rule 1.4 Communication
>
> (a) A lawyer shall:
> (1) promptly inform the client of any decision or circumstance with respect to which the client's informed consent, as defined in Rule 1.0(e), is required by these Rules;
> (2) reasonably consult with the client about the means by which the client's objectives are to be accomplished;
> (3) keep the client reasonably informed about the status of the matter;
> (4) promptly comply with reasonable requests for information; and
> (5) consult with the client about any relevant limitation on the lawyer's conduct when the lawyer knows that the client expects assistance not permitted by the Rules of Professional Conduct or other law.
> (b) A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation.

But communicating as a leader/manager isn't just about speaking to clients. It's also speaking to our colleagues and subordinates toward that end, there are two key aspects of being a leader that I want to elaborate upon — empathy and patience.

Empathy

Empathy is about listening on another level. It's not just hearing what someone is saying to you.

- Listen with your ears – what is being said, and what tone is being used? Scared? Note the key words and phrases that people use. Discuss it.
- Listen with your eyes – what is the person doing with his or her body while speaking?
- Listen with your instincts – do you sense that the person is not communicating something important?
- Listen with your heart – what do you think the other person feels?

A but part of being empathetic is putting yourself in the other person's shoes. Seeing their issue from their point of view. But the key extension of that concept, and a critical part of being a leader, is once you "see" why others believe what they believe, acknowledge it. Validate the other person's perspective. Now, remember — *acknowledgement* does not always equal *agreement*. You can accept that people have different opinions from your own and that they may have good reason to hold those opinions.[9] Validation only requires that you acknowledge those opinions, not that you accept them. You might, for instance, think the person holding the particular opinion is mistake and you might consult with them and ask them to reconsider. But the validation part of the equation is a key part of the overall advisory/leadership process.

Patience

The second aspect of communication that I want to touch on here, is patience. There are two parts to this effort — patiently listening and patiently leading.

Proper communication, and ultimately effective management, depends as much on listening as it does on speaking. But the former concept is much easier said than done. As lawyers, our inclination is to be the one doing the talking. That tendency, however, often acts as an obstacle to effective leadership. Here are some tips for patiently listening and leading…and a bit about why they are important:

---

[9] https://www.mindtools.com/pages/article/EmpathyatWork.htm, last checked 2/21/2022.

- Patiently Listening
  - Let them speak without being cut off. Just don't interrupt.
  - Don't step on the end of their sentences. Let them finish, even if it's long and drawn out.
  - If they never shorten up, then you could have a talk with them about that. But explaining to them that they talk too much is different from cutting them off mid-sentence.
  - Let them vent even if they are wrong about something
    - Here's why this is important: People need to feel as though they are being HEARD.
    - If you want them to follow you, learn from you, be loyal to you, they need to feel as though their concerns, feelings, etc., are being heard. Listening patiently gives them that sense of satisfaction.

- Patiently Leading
  - It's also about interruption, but in the larger sense. You need to be patient when someone executes their job.
  - Allow people to fail. As long as there will not be damage to the client, let them make mistakes. *[CAVEAT: As a lawyer it's critical that you consider this carefully because we have both ethical and malpractice concerns when we (or our team members) make mistakes. I'm not talking about mistakes that affect the misrepresentation — I'm referring to harmless errors that can be teachable moments. Coordinate with your risk management counsel and your own supervisors if necessary in this regard].*
    - Just like you don't want to interrupt their sentences, don't interrupt their execution.
    - Then, use those mistakes as teachable moments.
    - When they make a mistake, don't rub their nose in it.
      - Helpful tip: Instead of saying, "This is how you should have done it," Asking them why they did it their way. Then ask them what they think of your alternative.
      - That's the difference between leading and dictating.

HOUR THREE — TECHNOLOGY

So you've heard of this Chat GPT thing? I guess that means we should talk about it. Of course, this program isn't only about Chat GPT. To properly understand the ethics issues in that program, we actually have to go a little deeper. So in this program we'll be talking about the different ethics issues that impact both Chat GPT, artificial intelligence (generally), and a few other new technologies that are relevant to the discussion of generative AI.

1. The more things change, the more they stay the same.

a. Yesterday's standard.

There are a myriad of technologies being used in the practice of law today. Whether it's email, texting, cloud storage, software as a service (SaaS), or artificial intelligence in its many forms, there's one common concern. With each technology we are moving data. Whether we are moving data from one person to another or moving it into the cloud, moving it to a software system so that system can process the data, it doesn't matter. It's all about moving data. In each case, we are concerned about the channels upon which that data travels—the highways our information rides along to get from place to place. When we take that information and put it on the Internet to move it we use the proverbial information superhighway.

The key question we need to ask ourselves is whether that highway is secure. Can anyone jump onto it and intercept the data we're moving? What about getting onto that highway to begin with? Just like a car uses an onramp to access a highway, you plug a cable into your computer and that carries your information onto the Internet. And what about the destination. Once you get there (the cloud, SaaS) is our data safe there?

Think about how this all started — using a wireless to move the information from your computer to the Internet. But if we use that type of a wireless onramp to the information superhighway, we have security issues. The data becomes vulnerable once we transmit it

through the air. By connecting to a wireless router we essentially open up a door to our computer and invite other people to come in and see whatever we have loaded onto our computers. The whole question of wireless access is also raised when we talk about cell phones and tablets. Those devices access the Internet and transmit information using unsecured networks as well.

Not only do we have issues of moving data (transmission), but we also have issues about situations where you move information to another place and leave it there- to store it. Cloud storage companies/websites end up storing the data on their own servers (in the "cloud"). Similarly, programs known as Software as a Service (SaaS) invoke all of the problems discussed because you are sending data to another company that is used in their programs, thus creating transmission issues, wireless problems and storage concerns. Not sure what "the cloud" is all about? The Pennsylvania Bar Association Committee on Legal Ethics and Professional Responsibility explained these technologies clearly when it stated:

> If an attorney uses a Smartphone or an iPhone, or uses web-based electronic mail (e-mail) such as Gmail, Yahoo!, Hotmail or AOL Mail, or uses products such as Google Docs, Microsoft Office 365 or Dropbox, the attorney is using "cloud computing." While there are many technical ways to describe cloud computing, perhaps the best description is that cloud computing is merely "a fancy way of saying stuff's not on your computer."[10] From a more technical perspective, "cloud computing" encompasses several similar types of services under different names and brands, including: web-based e-mail, online data storage, software-as-a-service ("SaaS"), platform-as-a-service ("PaaS"), infrastructure-as-a-service("IaaS"), Amazon Elastic Cloud Compute ("Amazon EC2"), and Google Docs."[11]

Fast forward now to generative AI like Chat GPT. It's the same concern. Chat GPT becomes valuable when you use it to process your client's information. You ask it questions

---

[10] Pennsylvania Bar Association Committee on Legal Ethics and Professional Responsibility Formal Opinion 2011-200, at 1, citing, Quinn Norton, "Byte Rights," Maximum PC, September 2010, at 12.

[11] Pa Opinion 2011-200 at 1

about your case so you can find some sort of answers — research, novel legal ideas, whatever. In order to get valuable answers, you need to give it specific information. That specific information is going to be client information. And once you move that client information to anywhere — the cloud, Chat GPT, whatever — the vulnerabilities of all of those technologies implicate the same ethical issues: the potential release or disclosure of confidential information (Rule 1.6), the potential loss of client information/property (a failure to safeguard client property per Rule 1.15), and the duty to supervise the vendors (Rule 5.3).

b. Yesterday's standard, applicable today.

It has long been established that lawyers could send unencrypted email regarding client matters, but that wasn't always the case. When the technology was first developed, the powers that be were opposed to permitting such email communication. However, things changed in the late 90s.

The ABA issued a formal opinion in 1999 which stated that there is a reasonable expectation of privacy despite the risk of interception and disclosure. The key development was that legislation was enacted making the interception of email a crime. In its Opinion, the ABA stated:

> "The Committee believes that e-mail communications, including those sent unencrypted over the Internet, pose no greater risk of interception or disclosure than other modes of communication commonly relied upon as having a reasonable expectation of privacy. The level of legal protection accorded e-mail transmissions, like that accorded other modes of electronic communication, also supports the reasonableness of an expectation of privacy for unencrypted e-mail transmissions. The risk of unauthorized interception and disclosure exists in every medium of communication, including e-mail. It is not, however, reasonable to require that a mode of communicating information must be avoided simply because interception is technologically possible, especially when unauthorized interception or dissemination of the information is a violation of law. The Committee concludes, based upon current technology and law as we are informed of it, that a lawyer sending confidential client information by unencrypted e-mail does not

violate Model Rule 1.6(a) in choosing that mode to communicate. This is principally because there is a reasonable expectation of privacy in its use."[12]

States, of course, followed suit and permitted the use of unencrypted email in the practice of law. What's key here is that we see the standard clearly— the reasonable expectation of privacy. It's important to understand the standard/rationale for permitting such email communications, because it continues to be relevant today. As new technologies are developed, the authorities apply the same reasoning. Consider the recent furor over gmail and other free email services.

In its Opinion 820, the New York State Bar Association opined about those free email systems.[13] The systems of yore were a concern because of the business model that the systems use to keep the service free. Here's how they worked: in return for providing the email service, "the provider's computers scan e-mails and send or display targeted advertising to the user of the service. The e-mail provider identifies the presumed interests of the service's user by scanning for keywords in e-mails opened by the user. The provider's computers then send advertising that reflects the keywords in the e-mail."[14] The obvious problem is that if a lawyer was using the email system for client work, then that lawyer was allowing the provider to scan confidential information.

When considering whether these new email systems would be permitted, the NY authorities first considered the rationale for permitting email back in the 90s. Email was allowed because, "there is a reasonable expectation that e-mails will be as private as other forms of telecommunication and…therefore…a lawyer ordinarily may utilize unencrypted e-mail to

---

[12] ABA Commission on Ethics and Professional Responsibility Formal Opinion 99-413

[13] New York State Bar Association Committee on Professional Ethics Opinion 820 – 2/8/08

[14] NYSBA Op. 820 at 2

transmit confidential information.[15] They applied that same reasoning to the question of free emails.

You'd think that the authorities would have banned the emails, given that their content was being read by the email system, right? Wrong. Even though the email messages in the system were scanned, the opinion noted that humans don't actually do the scanning. Rather, it's computers that take care of that task. Thus, they stated that "Merely scanning the content of e-mails by computer to generate computer advertising…does not pose a threat to client confidentiality, because the practice does not increase the risk of others obtaining knowledge of the e-mails or access to the e-mails' content."[16]

What the opinion is basically saying is that there continued to be a reasonable expectation of privacy in those email systems. Maybe the better way to phrase it is a reasonable expectation of "confidentiality," but the idea is the same (more on Rule 1.6, Confidentiality, later).

That ethical standard continued to be relevant and we saw it being applied later to a google product. On September 21, 2018 the Wall Street Journal reported that Google shares Gmail information with its app developers. But what's important is the type of information that's being shared and who viewed it. The WSJ article revealed that:

> Google Inc. told lawmakers it continues to allow other companies to scan and share data from Gmail accounts…the company allows app developers to scan Gmail accounts… outside app developers can access information about what products people buy, where they travel and which friends and colleagues they interact with the most. In some cases, employees at these app companies have read people's actual emails in order to improve their software algorithms.[17]

---

[15] NYSBA Op. 820 at 1

[16] NYSBA Op, 820 at 2

[17] https://www.wsj.com/articles/google-says-it-continues-to-allow-apps-to-scan-data-from-gmail-accounts-1537459989 last checked 7/3/2023.

Did you get that last part? There are real human beings who are reading the contents of Gmail messages. What we know from NY Opinion 780 is that if human beings are reading the lawyer emails, then lawyers no longer have a reasonable expectation of privacy in Gmail.

Sure, we lack some specific data about which emails were read, but that doesn't change the conclusion. We might not know if lawyers' messages in particular were included in the messages that were scanned. But that's sort of exactly the problem — we don't know. And we don't have any way to control or restrict the app developers from reading anyone's emails, including our practice-related emails. Because of that reality I don't think that lawyers have a reasonable expectation of privacy in using Gmail any more. Our duty to protect client confidences set forth in Rule 1.6 precludes us from using the service. I'll tell you the truth, it actually looks like no one — lawyer nor otherwise — has a reasonable expectation of privacy with the platform. That's why I think lawyers need to stop using Gmail for practice related matters immediately.

The same standard is relevant today. When lawyers use generative AI like Chat GPT, we put our client information into the system. Open source systems which are trained on the internet at large take the information that's fed into it and use it in it's processing going forward. The Enterprise DNA blog explained that, "Chat GPT logs every conversation, including any personal data you share, and will use it as training data. Open AI's privacy policy states that the company collects personal information included in 'input, file uploads, or feedback' users provide to Chat GPT and its other services. The company's FAQ explicitly states that it will use your conversations to improve its AI language models and that your chats may be reviewed by human AI trainers."[18]

---

[18] https://blog.enterprisedna.co/is-chat-gpt-safe/#:~:text=No%2C%20Chat%20GPT%20is%20not%20confidential.&text=The%20company%27s%20FAQ%20explicitly%20states,reviewed%20by%20human%20AI%20trainers last checked July 2, 2023.

You can see how ye olde Email standard is still relevant. Lawyers do not have an expectation of privacy if we put our client information into generative AI programs alike Chat GPT. Similarly, we also happen to violate Rule 1.6…

c. Yesterday's standards, expanded and applicable in the future.

i. Confidentiality and the Cloud. The Reasonable Care Standard

The early decisions that addressed technology didn't always talk about "cloud computing" in particular, but they set the standard that would be followed when that technology arrived. Thus, the State of Nevada addressed the ability of lawyers to store confidential client information and/or communications in an electronic format on a server or other device that is not exclusively in the lawyer's control.[19] The Committee found that it was ethically permissible and stated that, "If the lawyer acts competently and reasonably to ensure the confidentiality of the information, then he or she does not violate [the rules] by simply contracting with a third parity to store the information…"[20]

The Committee said that the duty to save files on third party servers is the same as the duty to safeguard files that are put into third party warehouses, so contracting for such storage is not a per se confidentiality violation.[21] The lawyer wasn't strictly liable for an ethics violation "even if an unauthorized or inadvertent disclosure should occur".[22] Instead, the question was whether they exercised proper care. They articulated a standard that would be repeated in many following opinions when they said, "The lawyer must act competently and reasonably to

---

[19] State Bar of Nevada, Standing Committee on Ethics and Professional Responsibility,Formal Opinion No. 33, February 9, 2006, at 1.

[20] Nevada Opinion No. 33, at 1.

[21] Nevada Opinion No. 33, at 1.

[22] Nevada Opinion No. 33, at 1.

safeguard confidential client information and communications from inadvertent and unauthorized disclosure."[23]

Similarly, New Jersey evaluated a technologically related issue— whether a lawyer can scan client files to a PDF, then archive them electronically and store those documents on the web.[24] Just like in Nevada, the concern was that Rule 1.6 requires "that the attorney 'exercise reasonable care' against the possibility of unauthorized access to client information."[25] The New Jersey Committee echoed the Nevada findings and stated that,

> "Reasonable Care…does not mean that "the lawyer absolutely and strictly guarantees that the information will be utterly invulnerable against all unauthorized access…What the term 'reasonable care' means in a particular context is not capable of sweeping characterizations or broad pronouncements." at 3.

Given the changing nature of technology, the New Jersey Committee was reluctant to make a particularly bold decision but they did provide some elaboration of what constituted "reasonable care." They stated that,

> "'The Touchstone in using 'reasonable care' against unauthorized disclosure is that: (1) the lawyer has entrusted such documents to an outside provider in circumstances in which there is an enforceable obligation to preserve confidentiality and security, and (2) use is made of available technology to guard against reasonably foreseeable attempts to infiltrate the data. If the lawyer has come to the prudent professional judgment he has satisfied both these criteria, then 'reasonable care' will have been exercised." at 5

That phrase, "reasonably foreseeable" was an indication of things to come. In fact, the standard evolved in a decision out of Maine. Maine agreed that the lawyer needs to take reasonable steps to protect confidentiality but they went further and they stated that,

> "the lawyer would be well-advised to include a contract provision requiring the contractor to inform the lawyer in the event the contractor becomes aware of any inappropriate use

---

[23] Nevada Opinion No. 33, at 1.

[24] State Bar of New Jersey, Supreme Court Advisory Committee on Professional Ethics, Opinion 701, April 10, 2006, 15 N.J.L. 897 April 24, 2006, at 2

[25] NJ Opinion 701, at 3.

> or disclosure of the confidential information. *The lawyer can then take steps to mitigate the consequences and can determine whether the underlying arrangement can be continued safely.* (emphasis added). at 2

This is the first time we see an extended affirmative duty on the lawyer's part. Maine set forth the idea that the lawyer's duty is ongoing and that there may be a time where a lawyer needs to actually take some action to protect the client information.

Arizona reviewed a question that was analogous to cloud storage and added a further elaboration of what it meant to be exercising reasonable care. Arizona said that if you're going to use online storage sites, Competence (Rule 1.1) demands that you understand them. Specifically they stated that "the competence requirements…apply not only to a lawyer's legal skills, but also generally to 'those matters reasonably necessary for the representation..' Therefore, as a prerequisite to making a determination regarding the reasonableness of online file security precautions, the lawyer must have, or consult someone with, competence in the field of online computer security."[26] In other words, in order to show that you're exercising reasonable care, you need to understand the systems or associate yourself with someone who has that understanding.

And there's something more— here we see a further expansion of the affirmative duty. Not only must we take reasonable precautions to protect confidentiality and security of client information, but, the committee acknowledged that as technology changes, certain protective measures might become obsolete.[27] Thus, the Committee warned that "As technology advances occur, lawyers should periodically review security measures in place to ensure that they still reasonably protect the security and confidentiality of the clients' documents and information."[28]

---

[26] State Bar of Arizona, Opinion 09-04, 12/2009, at 1.

[27] Arizona Opinion 09-04 at 2.

[28] Arizona Opinion 09-04 at 1-2.

Thus, there is a continuing obligation to revisit the reasonability of the security that our vendors are utilizing. In other words, we can't take the "stick our heads in the sand approach".

A year later, the State of Alabama agreed and stated that,

> "Additionally, because technology is constantly evolving, the lawyer will have a continuing duty to stay abreast of appropriate security safeguards that should be employed by the lawyer and the third-party provider. If there is a breach of confidentiality, the focus of any inquiry will be whether the lawyer acted reasonably in selecting the method of storage and/or the third party provider."[29]

In the same year, the New York Bar Association elaborated on that idea. In Opinion 842 they evaluated whether a lawyer could use an online data storage system to store and back up client confidential information. Like the other states that opined on the topic, they answered in the affirmative, subject to the same confidentiality concerns. They also confirmed the ongoing nature of the lawyer's duty if one were to make use of these systems. They stated:

> "10. Technology and the security of stored data are changing rapidly. Even after taking some or all of these steps (or similar steps), therefore, the lawyer should periodically reconfirm that the provider's security measures remain effective in light of advances in technology. If the lawyer learns information suggesting that the security measures used by the online data storage provider are insufficient to adequately protect the confidentiality of client information, or if the lawyer learns of any breach of confidentiality by the online storage provider, then the lawyer must investigate whether there has been any breach of his or her own clients' confidential information, notify any affected clients, and discontinue use of the service unless the lawyer receives assurances that any security issues have been sufficiently remediated. See Rule 1.4 (mandating communication with clients); see also N.Y. State 820 (2008) (addressing Web-based email services)."[30]

In the following, far less earth-shattering paragraph, the New York authorities also noted the need for lawyers to stay abreast of the law regarding technology. "Not only technology itself but also the law relating to technology and the protection of confidential communications is changing rapidly. Lawyers using online storage systems (and electronic means of

---

[29] Alabama Ethics Opinion 2010-02 at 16

[30] New York State Bar Association Opinion 842 (9/10.10) at 4.

communication generally) should monitor these legal developments, especially regarding instances when using technology may waive an otherwise applicable privilege. *[citation omitted]*."[31]

Do I even need to make the connection to Chat GPT? When you use that system, you give them your client information. It's the functional equivalent of storing it with them. Thus, all of the ethical standards that govern cloud computing apply to Chat GPT as well. That's why I say that not much has changed. The same holds true for Rule 1.15…

ii. Our Fiduciary Duty Under 1.15

In North Carolina we see an opinion that reveals the second of the two major ethical concerns with using cloud-based systems/software. That's the need to protect our client's information with the care required of a fiduciary as set forth in Rule 1.15.

Most people hear the Rule number "1.15" and think about trust accounts. It's true that the rule is most often invoked in our discussion about our client's money, but the rule actually has broader implications. Rule 1.15 governs our responsibilities with our client's property and money is just one type of client property that we might hold. Another type of property is the client's file.

The hard copy of your client's file is the client's property and we also know that Rule 1.15 mandates that we take steps to safeguard that property. When you think about it, however, the digital version of your client's file is also their property—you're simply holding it in computerized form. Any information about your client matter is part of their "file." Thus, if we release that to another individual (like a cloud storage vendor, or a generative AI program) we need to make sure that we're taking steps to safeguard that client property appropriately. That invokes Rule 1.15, which is why the North Carolina opinion states, "Rule 1.15 requires a lawyer to preserve client property, including information in a client's file such as client documents and lawyer work

---

[31] New York State Bar Association Opinion 842 (9/10.10) at 4.

product, from risk of loss due to destruction, degradation, or loss. See also RPC 209 (noting the "general fiduciary duty to safeguard the property of a client")."[32]

In the end, the North Carolina authorities didn't provide any new ethical ideas, rather they simply confirmed that using SaaS (cloud computing), in particular, was not a violation. Specifically, they stated, "Lawyers can use SaaS, "provided steps are taken effectively to minimize the risk of inadvertent or unauthorized disclosure of confidential client information and to protect client property, including the information in a client's file, form risk of loss." But when you apply that to programs like Chat GPT you have a problem. When you give client information to those types of programs you have no way to "minimize the risk of inadvertent or unauthorized disclosure of confidential client information." Zero. There is no way to minimize the risk. In fact, you have to assume that the information will be spit out somewhere else at some time because the system told you that's a possibility.

Let's address something here — there are some systems that purport to give you an option to "opt out" of sharing your client data. Some systems might give us the option to simply "disallow" the collection and/or dissemination of that data. If lawyers actually did opt out, then that might change the calculation. But there are two problems with that. (1) trusting the tech companies to honor that pledge and (2) forgetting to end the collection/dissemination altogether.

Regarding the first, you'll have to forgive me for not trusting big tech, but consider the following excerpt from the website The Verge in their article, "Amazon confirms it holds on to Alexa data even if you delete audio files being used' by Makena Kelly and Nick Statt:

> Amazon has admitted that it doesn't always delete the stored data that it obtains through voice interactions with the company's Alexa and Echo devices — even after a user chooses to wipe the audio files from their account. The revelations, outlined explicitly by Amazon in a letter to Sen. Chris Coons (D-DE), which was published today and dated

[32] The North Carolina State Bar, 2011 Formal Ethics Opinion 6, Issued in January 27, 2012.

June 28th, sheds even more light on the company's privacy practices with regard to its digital voice assistant.[33]

Regarding the second — forgetting to deny/end the collection and dissemination of that information — it's really just a question of lawyers not having that heightened sense of awareness I'm always talking about.

We are inundated with requests to share information. Every device/program we use asks us if we can share data and we simply click "yes" oftentimes without even thinking. The constant barrage of such requests is likely desensitizing us to the dangers of granting those request. At some point we're going to end up sharing data for a device or system that is going to provide out client data to someone who shouldn't be seeing it.

iii. The Extension of our Duty to Supervise.

The day-to-day realities of the practice reveal that lawyers are not the only individuals in the office about whom we must be concerned when we decide to use technology. The commentary to Rule 1.6 confirms that: "[16]…A lawyer must act competently to safeguard information relating to the representation of a client 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." Various states have expanded upon that concept and discussed our larger responsibility to train our non-lawyer staff.

In an opinion we discussed earlier, the Maine Committee confirmed that the primary responsibility for confidentiality remains with the lawyer, but they also noted that the Maine rule "implies that lawyers have the responsibility to train, monitor, and discipline their non-lawyer staff in such a manner as to guard effectively against breaches of confidentiality. Failure to take steps to provide adequate training, to monitor performance, and to apply discipline for the

---

[33] https://www.theverge.com/2019/7/3/20681423/amazon-alexa-echo-chris-coons-data-transcripts-recording-privacy, last checked 1/14/2022.

purposes of enforcing adherence to ethical standards is grounds for concluding that the lawyer has violated [the rule]."[34]

Plus, our duties extend beyond keeping an eye on our in-house nonlawyer staff. The foundation for that was laid before the technology era when the Oregon State Bar addressed whether a lawyer could use a recycling service to dispose of client documents. The issue was whether doing so violated the rule on confidentiality because you would be exposing confidential client information to the recycling vendor. The opinion held that, "as long as Law Firm makes reasonable efforts to ensure that the recycling company's conduct is compatible with Law Firm's obligation to protect client information," using the service is permissible.[35] They further stated that "reasonable efforts include, at least, instructing the recycling company about Law Firms duties pursuant to Oregon RPC 1.6 and obtaining its agreement to treat all materials appropriately."[36] This is exactly the sentiment set forth by other bars regarding cloud computing vendors.

The Maine Committee noted that the technology vendor needs to be supervised as well. While the lawyer doesn't directly train or monitor the service provider employees, "the lawyer retains the obligation to ensure that appropriate standards concerning client confidentiality are maintained by the contractor."[37]

The Oregon and Maine opinions marked the beginning of a trend, about which all lawyers must be aware. Over the past several decades we've seen states expand upon the duty for lawyers to be responsible for non-lawyers who are working for the firm, but not necessarily

---

[34] Maine Board of Overseers of the Bar, Opinion #194, Issued June 30, 2008, at 1-2.

[35] Oregon State Bar, Formal Opinion No. 2005-141, August 2005, at 386

[36] Oregon Opinion 2005-141 at 386.

[37] Maine Board of Overseers of the Bar, Opinion #194, Issued June 30, 2008, at 2.

inside the firm's office. This was further exhibited in North Carolina's Formal Ethics Opinion 6, in which they stated,

> "Although a lawyer may use nonlawyers outside of the firm to assist in rendering legal services to clients, Rule 5.3(a) requires the lawyer to make reasonable efforts to ensure that the services are provided in a manner that is compatible with the professional obligations of the lawyer. The extent of this obligation when using a SaaS vendor to store and manipulate confidential client information will depend upon the experience, stability, and reputation of the vendor. Given the rapidity with which computer technology changes, law firms are encouraged to consult periodically with professionals competent in the area of online security."[38]

New Hampshire went a little further and let us know that we can't pass the buck when it comes to the tech vendors. They made is clear that the duties of confidentiality and competence are ongoing and not delegable:[39]

> "When engaging a cloud computing provider or an intermediary who engages such a provider, the responsibility rests with the lawyer to ensure that the work is performed in a manner consistent with the lawyer's professional duties. Rule 5.3 (a). Additionally, under Rule 2.1, a lawyer must exercise independent professional judgment in representing a client and cannot hide behind a hired intermediary and ignore how client information is stored in or transmitted through the cloud.[40]

A short while ago, the ABA chimed in on the topic. In a batch of amendments, the ABA made a change to two letters in the title of Rule 5.3-- that's right, I said two letters in the *title* -- and that change has profound implications. Rule 5.3 used to be called, "Responsibilities Regarding Nonlawyer Assistants." However, how it's called, "Responsibilities Regarding Nonlawyer Assistance." Did you catch that? The last two letters of the final word-- "Assistants" is now "Assistance." This is a big deal because it reflects a growing trend in the world of ethics. Yes, we are responsible for supervising our own staff, but today that duty extends to other parties like those that we would have once called "independent contractors." Anyone that we

---

[38] North Carolina's 2011 Formal Ethics Opinion 6

[39] New Hampshire Opinion 2012-13/4, at 4.

[40] New Hampshire Opinion 2012-13/4, at 3.

use in assistance, like vendors, are parties that we now have a duty to supervise. We get further guidance in this regard from new Comments [3] and [4] in Rule 5.3.

What we notice from those comments is that this change was brought about mostly because (a) lawyers now outsource many of the tasks that used to be completed in house and (b) there is an increased reliance on cloud storage and other technology-related vendors. Thus, the comments tell us that we must supervise nonlawyers outside the firm that we use for investigations, document management, cloud storage, etc., and the Comment also provides factors that should be considered when determining the extent of our obligations in these circumstances.

The new technologies that are powered by AI are no different from a supervision standpoint. We simply can not delegate our ability to supervise those technologies simply because we have vendors who assist us in utilizing them. All of the opinions regarding the lawyer's duty of supervision apply to these new technologies as well.

iv. The Emerging Affirmative Duty to Understand, Anticipate, and Act

I've tried to take the information that's been provided by the various state opinions and distill it down to some workable direction to attorneys. Here's how it looks to me:

All of these opinions make clear is that we need to be competent and protect client confidentiality. In order to do that we need to understand the technological systems, understand the security precautions that the vendors use, supervise the vendors appropriately, ensure that the terms of service are adequate, and remember that the review of all of the foregoing is a continuing duty (plus some other stuff, but those are the biggies).

What's clear is that the opinions have created a significant affirmative duty for lawyers who choose to use cloud systems. *We have an ongoing obligation to understand, anticipate, and act.* We must understand the technology, the security, and the law. We must be able to anticipate security issues, problems presented by our nonlawyer staff, confidentiality concerns,

and everything else. And if the situation requires it, we must act. We may be forced to change vendors, for instance, if we think our client's information is vulnerable. We may need to demand that vendor change some protocol. It could be anything.

The point is that we can't sit idly by. Ignorance is not bliss, it's an ethical violation. If we are going to utilize these systems we need to continually stay up to date on all relevant variables. It's an active, ongoing process.

2. Chatbots: the legal marketing device that could get you in trouble

Chatbots are used in legal marketing to help lawyers find valuable clients. The technology is basically a computer program that is powered by artificial intelligence and it simulates conversation with people. Potential clients who visit a firm's site can type questions and comments into a chatbox and, when doing so, they think they are speaking with a real person (or at least it's supposed to seem that way). Meanwhile, the bot collects contact info as well as other information about the potential client's case, analyzes it, and gives that info to the lawyer. The chatbot companies say that their AI allows them to sift out the tire kickers, identify the valuable prospects, and improve conversion rates from visitors to actual clients.

The chatbots are provided by tech vendors. A lawyer contracts with a vendor that offers the chatbot software, the vendor provides a bit of code that is inserted into the lawyer's website, and the chatbot becomes a part of the lawyer's site. Someone coming to the website wouldn't know that another vendor is operating it— it simply looks like a chat box that is part of the lawyer's website.

Using a chatbot isn't necessarily a problem. What you need to be concerned about is the nature of the exchange between the bot and the potential client. Of course, it's a problem if a chat bot engages in conversation with a potential client and dispenses legal advice. But that's not likely to happen because that's not what the bots do. They are just supposed to be weeding out the garbage contacts from the good prospects. But in order to do that, the

chatbot needs to ask the prospect some questions, and evaluate the data. That is where the problem could arise…

There is a conversation that goes on between the bot and the prospect. During that conversation the prospect will be providing information about their case. What we need to worry about is the potential that people who visit the lawyer's site and engage in a conversation with the chatbot end up being considered "prospective clients" under Rule 1.18. If they do attain that status, the lawyer could have conflict problems. To see what I mean, first understand how the rule works.

a. <u>How Rule 1.18 Works</u>

Rule 1.18 says that if a person "consults with a lawyer about the possibility of forming a client-lawyer relationship" they could be a prospective client. All they need to do is *consult* about the *possibility* of forming the lawyer client relationship. But what does that mean? Why should a lawyer care if someone is technically considered a "prospective client?"

First, you can't tell anyone about the information that the prospective client gave you. Rule 1.18(b) explains that "Even when no client-lawyer relationship ensues, a lawyer who has learned information from a prospective client shall not use or reveal that information…" Second, you might be conflicted out of representing people in the future. Even if you don't take the prospective client and never work on their matter, subsection (c) says that if you received information from the prospective client that could be significantly harmful to that person, and some time in the future a person approaches you to represent that new person against the prospective client in the same matter, you might not be permitted to so so. You would be conflicted out of the representation.

That could be devastating. Think about it— if you have a consultation with someone about a lucrative matter and you decide not to take their case…but later you are approached by someone who wants you to represent them in that very case you can't take that other client. You could be forced to forego a lot of money in fees.

b. The problem with chatbots

So back to the bots and Rule 1.18. What's important is the trigger for becoming a prospective client, and as you saw from the rule above, the trigger is a consultation. The key question, of course, is, when does something rise to the level of a *consultation?* The answer is that it depends on the circumstances. But, in my opinion, the key circumstances to focus on are (1) what your website says and (2) the level of detail in the chatbot's communications.

If your website just lists your contact information you're going to be okay. If you simply put your information out there and someone sends you information about a case, that's not going create a prospective client relationship. Comment [2] confirms that: "…a consultation does not occur if a person provides information to a lawyer in response to advertising that merely describes the lawyer's education, experience, areas of practice, and contact information, or provides legal information of general interest." Basically, that comment is saying that if you simply tell someone that you exist and that you are qualified, it's not a "consultation." If someone replies in that situation, the person "communicates information unilaterally to a lawyer, without any reasonable expectation that the lawyer is willing to discuss the possibility of forming a client-lawyer relationship." That person, therefore, is not a prospective client.

However, you're going to have a problem if your website encourages people to offer information and your chatbot follows up by asking for information. The comment explains that "…a consultation is likely to have occurred if a lawyer…through the lawyer's advertising in any medium, specifically requests or invites the submission of information about a potential representation without clear and reasonably understandable warnings and cautionary statements that limit the lawyer's obligations, and a person provides information in response."

If your site specifically requests or invites a person to submit information about a potential representation, and your chat bot provides information in response, then you are risking the creation of a prospective client relationship. Obviously, the ethical danger is dependent upon the responsiveness of the chatbot because the rule says that you have to

"provide information in response." Well, the more lengthy, intense, and detailed the chatbot's responses, the more likely there will be a problem.

Oh, and don't get hung up on the fact that your chatbot is not a "person" under the rules. Personally, if the bot provides information I think a tribunal will see the software as an extension of the lawyer. Plus, if the AI software is doing its job correctly, the potential client should believe that they are actually communicating with a real person. For those reasons, I wouldn't be surprised if a tribunal concluded that the AI in the chatbot is the functional equivalent of a "person" for the purposes of the rule.

Of course, there is a huge get-out-of-trouble card. All you have to do is include the disclaimers set forth in the rule. If your site has "clear and reasonably understandable warnings and cautionary statements that limit the lawyer's obligations" as stated in Comment [2], you're probably ok. This, however, is a situation where you can win the ethical battle, but lose the overall war. What I mean by that is…what if this issue isn't raised in an ethics grievance? What if it is, instead, raised in a disqualification motion?

c. Win the ethical battle, but lost the disqualification war

Let's say you're in a medium sized firm that handles a variety of different types of matters. Your firm represents Business X and you've been their counsel on various issues for years. Your firm has a website that utilizes a chatbot to evaluate the strength of clients. You have language on the website that properly disclaims Rule 1.18. Someone visits your site and explains that they have a workplace discrimination claim. They provide details of the case to the chatbot. The bot inquiries further and the prospect provides more information, in fact, the client wants to make sure that the lawyer with whom they are chatting has a complete understanding of the case (maybe they don't know it isn't a computer) so they provide a lot of details.

The chatbot sends the info to the attorney at the firm responsible for reviewing the contacts made by the chatbot and that lawyer thinks that the prospect has a great case. After reviewing the information, the attorney contacts the prospect and learns that the adverse party

is Business X. However, the lawyer figures that the firm will probably be representing Business X in that matter because the firm does all of their work. As a result the firm doesn't take the potential client.

The prospect finds another lawyer, and they file suit against Business X. As the lawyer anticipated, the firm is representing Business X. The prospect's lawyer files a motion to disqualify you as counsel and you oppose it. You claim that there is no violation of the rule— the prospect never became a "prospective client" under Rule 1.18 because you had the proper disclaimer. And you're probably right. But there is a good chance that a judge will disqualify you anyway.

Remember, the judge isn't deciding discipline — the judge is deciding whether you should be disqualified. They don't necessarily care about the technicalities of the rules, they care about two things — the two things that are at the core of *every* conflict— loyalty and confidential information.

The critical question that the judge will ask was, *during the interaction the firm had with the prospect, did you learn confidential information from the other party?* And when the judge realizes that your chatbot gathered information that would ordinarily be considered confidential information and it was passed on to the lawyer in your firm for review, they're going to say you have a conflict and kick you out of the case. You're not going to be saved by the disclaimers because those disclaimers only helped you avoid discipline under Rule 1.18. In the disqualification context the court cares about loyalty and confidential information. And when it finds out that you were privy to a slew of details from the potential client's case, they will disqualify you.

d. <u>How to make chatbots safer</u>

All of this doesn't mean that chatbots can't be used, they just need to be used carefully. What can you do to make the chatbot safer? Here are 5 ideas:

(1) Use disclaimers

(2) Make sure the bot is just gathering information and not giving any information. And if it does give information, make sure it's super limited. Keep Comment [4] to Rule 1.18 in mind which states, "In order to avoid acquiring disqualifying information from a prospective client, a lawyer considering whether or not to undertake a new matter should limit the initial consultation to only such information as reasonably appears necessary for that purpose."
(3) Go over Rule 1.18 with the vendor supplying your chatbot. Make sure they understand it. also explain the disqualification issue. Remember, most tech vendors have no idea about the details rules like 1.18.
(4) Train the staff/lawyers in your office who are responsible for following up on the leads developed by the bot. Let them know about Rule 1.18 and the issue of disqualification.
(5) Create a process that limits the exposure the lawyers who review the information provided by the chatbots. It is possible to screen those attorneys per 1.18(d)(2). Here's what that section states, in part:

> (d) When the lawyer has received disqualifying information… representation is permissible if…(2) the lawyer who received the information took reasonable measures to avoid exposure to more disqualifying information than was reasonably necessary to determine whether to represent the prospective client; and (i) the disqualified lawyer is timely screened from any participation in the matter and is apportioned no part of the fee therefrom; and (ii) written notice is promptly given to the prospective client.

3. Attorney ethics in the meta verse.

The future is the metaverse. At least, that's what Facebook thinks. I mean, they changed their name to Meta in anticipation of the growth of that part of the internet. Since it appears to be a large part of life in the not-to-distant future, Rule 1.1 (Competence) demands that we understand what it is and the ethical implications that are posed to lawyers.

What is the metaverse? It's basically an alternate reality that exists on line. I gathered a few excerpts from some reputable online sources to explain the metaverse:

> *According to a Fast Company article, Dan Eckert, managing director, AI and emerging technology, PwC explained:*
>
> > An extended reality metaverse is still 3-5 years out: The metaverse—or should we say metaverses—has been around since the time of multiplayer computer games and even Second Life/AOL/Compuserve.
> > Yes, plural–there will not be just one–there will be many, each designed for focused communities, capabilities, and experiences. The Metaverse, as being shouted by everyone, is not shipping (yet), but we are starting to see the building blocks released every day.[41]
>
> *Bernard Marr explained in Forbes:*
>
> > Digitization, datafication and virtualization
> >
> > During 2020 and 2021, many of us experienced the virtualization of our offices and workplaces, as remote working arrangements were swiftly put in place. This was just a crisis-driven surge of a much longer-term trend. In 2022, we will become increasingly familiar with the concept of a "metaverse" – persistent digital worlds that exist in parallel with the physical world we live in. Inside these metaverses – such as the one proposed recently by Facebook founder Mark Zuckerberg – we will carry out many of the functions we're used to doing in the real world, including working, playing, and socializing. As the rate of digitization increases, these metaverses will model and simulate the real world with growing accuracy, allowing us to have more immersive, convincing, and ultimately valuable experiences within the digital realm. While many of us have experienced somewhat immersive virtual realities through headsets, a range of new devices coming to the market will soon greatly improve the experience offering tactile feedback and even smells. Ericsson, which provided VR headsets to employees working from home during the pandemic, and is developing what it calls an "internet of senses," has predicted that by 2030 virtual experiences will be available that will be indistinguishable from reality. That might be looking a little

[41] https://www.fastcompany.com/90704618/the-biggest-tech-trends-of-2022, last checked 1/12/2022.

> further ahead than we are interested in for this article. But, along with a new Matrix movie, 2022 will undoubtedly take us a step closer to entering the matrix for ourselves.[42]

Finally, from a CNBC article - "Investors are paying millions for virtual land in the metaverse" by Chris DiLella and Andrea Day:

> It's no secret the real estate market is skyrocketing, but the Covid pandemic is creating another little-known land rush. Indeed, some investors are paying millions for plots of land — not in New York or Beverly Hills. In fact, the plots do not physically exist here on Earth.
>
> Rather, the land is located online, in a set of virtual worlds that tech insiders have dubbed the metaverse. Prices for plots have soared as much as 500% in the last few months ever since Facebook announced it was going all-in on virtual reality, even changing its corporate name to Meta Platforms.
>
> "The metaverse is the next iteration of social media," said Andrew Kiguel, CEO of Toronto-based Tokens.com, which invests in metaverse real estate and non fungible token-related digital assets.[43]

The connection to attorney ethics goes beyond merely the need to be competent and understand the concept. It can also apply to our actions when we use the meta verse ourselves. Lawyers will surely participate, in a professional and personal capacity. I could envision lawyers having a virtual presence of some sort in the metaverse, I must admit that I don't know how that would look, but I'm sure it's going to happen. In addition, lawyers will participate in the metaverse in ways that were unrelated to the practice of law. The thing to remember is that no matter what type of presence we have in the metaverse, the ethics rules will still apply to your behavior.

Your behavior in the metaverse is going to be regulated by the disciplinary system in the real world. Any action you take as a practicing lawyer that occurs in the metaverse will be governed by the rules of attorney ethics. And it doesn't stop there. Even actions that are not related to the practice could be covered by the rules. If you steal something in the metaverse,

---

[42] https://www.forbes.com/sites/bernardmarr/2021/09/27/the-5-biggest-technology-trends-in-2022/?sh=4bafc07c2414, last checked 1/12/2022.

[43] https://www.cnbc.com/2022/01/12/investors-are-paying-millions-for-virtual-land-in-the-metaverse.html, last checked 1/17/2022.

you'll need to answer to Rule 8.4(b): "It is professional misconduct for a lawyer to (b) commit a criminal act that reflects adversely on the lawyers honesty, trustworthiness, or fitness as a lawyer in other respects." This isn't an alien concept- we all know that our personal behavior is within the purview of the ethics authorities. This is simply another part of our personal life, and we need to be aware that the long arm of the disciplinary system reaches into alternate universes as well as the real world.

Here's an interesting quirk that might arise in the metaverse. What if you assume an alternate personality. I'm going to guess that a lot of people who participate in the metaverse will become a character that's different from their true persona. It's just speculation on my part, but I have to believe that there are a lot of people who are looking forward to the metaverse as a way to escape from the life that they currently lead. But lawyers need to beware. Taking on an alternate identity could end up somehow violating Rule 8.4(c) — "It is professional misconduct for a lawyer to: (c) engage in conduct involving dishonesty, fraud, deceit or misrepresentation…"

4. More controversial uses of AI technology and the role lawyers should (?) play.

Let's consider some of the more controversial uses of the technology: predictive policing,[44], biases in algorithms[45] and surveillance uses like facial recognition[46].

a. Predictive Policing

One hot use for AI technology is called, "predictive policing" Nature.com explained,

> …police agencies hope to 'do more with less' by outsourcing their evaluations of crime data to analytics and technology companies that produce 'predictive policing' systems. These use algorithms to forecast where crimes are likely to occur and who might commit them, and to make recommendations for allocating police resources. Despite wide adoption, predictive policing is still in its infancy, open to bias and hard to evaluate.

---

[44] https://www.nature.com/articles/541458a, last checked 6/19/2021.

[45] https://www.nature.com/articles/d41586-018-05469-3, last checked 6/19/2021.

[46] https://www.nature.com/articles/d41586-019-03775-y, last checked 6/19/2021.

> Predictive models tie crimes to people or places. Offender-based modelling creates risk profiles for individuals in the criminal justice system on the basis of age, criminal record, employment history and social affiliations. Police departments, judges or parole boards use these profiles — such as estimates of how likely a person is to be involved in a shooting — to decide whether the individual should be incarcerated, referred to social services or put under surveillance. Geospatial modelling generates risk profiles for locations. Jurisdictions are divided into grid cells (each typically around 50 square metres), and algorithms that have been trained using crime and environmental data predict where and when officers should patrol to detect or deter crime.[47]

It doesn't take much to understand how this sort of programming could end up yielding discriminatory results. The very word "predictive" in the name of the technology gives an indication of the problem.

b. Biases in Algorithms

The final article from Nature.com that I'm going to quote today addresses the ethics issue with biases in algorithms. In an article entitled, "Bias detectives: the researchers striving to make algorithms fair", the website explained the concern that arises when AI algorithms are used to help…and how that could go awry.

> In 2015, a worried father asked Rhema Vaithianathan a question that still weighs on her mind. A small crowd had gathered in a basement room in Pittsburgh, Pennsylvania, to hear her explain how software might tackle child abuse. Each day, the area's hotline receives dozens of calls from people who suspect that a child is in danger; some of these are then flagged by call-centre staff for investigation. But the system does not catch all cases of abuse. Vaithianathan and her colleagues had just won a half-million-dollar contract to build an algorithm to help.
>
> Vaithianathan, a health economist who co-directs the Centre for Social Data Analytics at the Auckland University of Technology in New Zealand, told the crowd how the algorithm might work. For example, a tool trained on reams of data — including family backgrounds and criminal records — could generate risk scores when calls come in. That could help call screeners to flag which families to investigate.
>
> After Vaithianathan invited questions from her audience, the father stood up to speak. He had struggled with drug addiction, he said, and social workers had removed a child from his home in the past. But he had been clean for some time. With a computer assessing his records, would the effort he'd made to turn his life around count for nothing? In other words: would algorithms judge him unfairly?

c. The dangerous rise of the surveillance state

---

[47] https://www.nature.com/articles/541458a, last checked 6/20/2021.

If you're not aware of the ever-growing encroachment of the surveillance state, then you must live under a rock. But don't worry…no matter how well you're hidden under that boulder, they know where you are. Who are "they?"

QIUET — WE ASK THE QUESTIONS!!

All kidding aside, the concern about the surveillance state is no longer the thing of conspiracy theories. I'm not some aluminum-foil-hat-wearing eccentric. Rather, I'm a teacher who likes to watch how paradigms shift. And any review of credible news resources today reveals that we are in the midst of an important paradigm shift. The use of artificially intelligent surveillance technologies has expanded significantly, and those resources are becoming a primary part of the governmental toolkit across the globe. It's time for lawyers to start to consider all of this, and to think about what, if any, obligation we have as a practice.

A quick Google search reveals the extent to which people are being watched by the government these days. We saw surveillance technology employed during the COVID lockdowns. The Wall Street Journal reported about the experience of a man in Beijing: "Late one night recently, he received an automated phone call from Beijing authorities saying he had been in proximity to someone with a confirmed Covid infection, which means he can't go to public places until the health code on his phone turns green. That could involve two PCR tests and several days' wait."[48]

The use of technology to monitor people is certainly not limited to our devices. In an article entitled, "Chinese 'gait recognition' tech IDs people by how they walk " Dake Kang of the Associated Press reported:

---

[48] China's Lockdowns Prompt a Rethinking of Life Plans Among the Young by Liyan Qi and Shen Lu, May 29, 2022, https://www.wsj.com/articles/chinas-lockdowns-prompt-a-rethinking-of-life-plans-among-the-young-11653822000 last checked 7/8/2022.

> Chinese authorities have begun deploying a new surveillance tool: "gait recognition" software that uses people's body shapes and how they walk to identify them, even when their faces are hidden from cameras.
>
> Already used by police on the streets of Beijing and Shanghai, "gait recognition" is part of a push across China to develop artificial-intelligence and data-driven surveillance that is raising concern about how far the technology will go.[49]

Facial recognition technology is apparently being used in relatively nefarious ways in society today. In Nature.com authors Richard Van Noorden & Davide Castelvecchi wrote an article in 2019 entitled. "Science publishers review ethics of research on Chinese minority groups":

> Two science publishers are reviewing the ethics of research papers in which scientists backed by China's government used DNA or facial-recognition technology to study minority groups in the country, such as the predominantly Muslim Uyghur population.
>
> Springer Nature (which publishes Nature) and Wiley want to check that the study participants gave informed consent, after researchers and journalists raised concerns that the papers were connected to China's heavy surveillance operations in the northwestern province of Xinjiang. China has attracted widespread international condemnation — and US sanctions — for mass detentions and other human-rights violations in the province. The Chinese government says that it is conducting a re-education campaign in the region to quell what it calls a terrorist movement.
>
> 'We are very concerned about research which involves consent from vulnerable populations…'[50]

The use of this technology is by no means restricted to China. Quite the contrary, it's already being put into use across the globe. The MIT Technology Review explained how France is making great efforts to disseminate monitoring technology:

> Since 2015, the year of the Bataclan terrorist attacks, the number of cameras in Paris has increased fourfold. The police have used such cameras to enforce pandemic lockdown measures and monitor protests like those of the Gilets Jaunes. And a new

---

[49] https://apnews.com/article/china-technology-beijing-business-international-news-bf75dd1c26c947b7826d270a16e2658a last checked 7/7/2022.

[50] https://www.nature.com/articles/d41586-019-03775-y, last checked 1/17/2022.

> nationwide security law, adopted last year, allows for video surveillance by police drones during events like protests and marches.[51]

The technology has even expanded to the evaluation of DNA. NPR interviewed Yves Moreau, an engineer and professor at the Catholic University in Leuven, Belgium, and they discussed the use of DNA data in surveillance. They acknowledged that "DNA data has been used to track and identify alleged criminals for decades,"[52] But the concern is:

> [The technology] has been rolled out on a very large scale. And what we have seen is that this technology is being rolled out in particular in the west of China. And in 2016, 2017, blood samples from essentially the entire population, people 12 to 65 in Xinjiang, was collected and potentially put in that database. And it can be part of a broader system of what we call total surveillance.[53]

The use of technology in this way made the professor concerned about its relationship to historical acts of genocide:

> I'm extremely concerned about this because in history, actually, if you look back in the first half of the 20th century, German and then Belgian colonists in Rwanda and Burundi actually went there, and they were using pseudoscientific ideas about race and assigned people to a particular ethnicity. That actually was a significant factor in genocides. And the risk for this in the midterm is actually really worrying.[54]

The paradox is that there are good uses for the technology.

In Fortune magazine, author Jeremy Kahn evaluated whether Artificial Intelligence could be used to prevent future mass shootings. While the author was skeptical it could work, he could not rule the possible benefits of using AI in this context. He explained that one option is to "use computer vision algorithms to try to detect people attempting to carry weapons on to school grounds. There are already a number of A.I. software and CCTV camera vendors that claim to

---

[51] MIT Technology Review, "Marseille's battle against the surveillance state" by Fleur Macdonald, June 13, 2022, https://www.technologyreview.com/2022/06/13/1053650/marseille-fight-surveillance-state/ last checked 7/8/2022.

[52] https://www.npr.org/2019/12/07/785804791/uighurs-and-genetic-surveillance-in-china last checked 7/8/2022.

[53] https://www.npr.org/2019/12/07/785804791/uighurs-and-genetic-surveillance-in-china last checked 7/8/2022.

[54] https://www.npr.org/2019/12/07/785804791/uighurs-and-genetic-surveillance-in-china last checked 7/8/2022.

offer ‘gun detection’ algorithms.”[55] Another possible use of AI technology is “to create "smart guns" that are fitted with cameras and A.I. software. Such a system could be set to detect whether the person being aimed at is a child and prevent the gun from being fired.”[56] He also noted that "it is possible that this kind of A.I. could help flag troubled individuals who are at risk of committing violence.”[57]

In the article, Mr Kahn acknowledges that there are serious questions about the practical effectiveness of these systems. But that’s not really relevant for our discussion in this program. My purpose for bringing these ideas up is not to debate the efficacy of these systems, rather, it’s to point out that the existence of AI motoring capabilities is not a problem, per se. There are certainly a huge number of potential societal benefits of the technology.

Using the AI powered technology for beneficial purposes — like tracking domestic terrorists, for example — is something few people would probably oppose. The problem is that once you give the government the authority to use the technology in tracking bad guys, you let them employ that technology whenever they thing they’re going after bad guys. And they get to determine who the “bad guys” are. Wired magazine reported on research by the Surveillance Technology Oversight Project (“STOP”). Their conclusion: “A surveillance state built to track certain types of behavior can easily, and inevitably, be adapted to other ends.”[58]

---

[55] "After Uvalde: Could A.I. prevent another school shooting?” By Jeremy Kahn, May 31, 2022, https://fortune.com/2022/05/31/ai-prevent-uvalde-mass-school-shooting/ last checked 7/8/2022.

[56] "After Uvalde: Could A.I. prevent another school shooting?” By Jeremy Kahn, May 31, 2022, https://fortune.com/2022/05/31/ai-prevent-uvalde-mass-school-shooting/ last checked 7/8/2022.

[57] "After Uvalde: Could A.I. prevent another school shooting?” By Jeremy Kahn, May 31, 2022, https://fortune.com/2022/05/31/ai-prevent-uvalde-mass-school-shooting/ last checked 7/8/2022.

[58] “The Surveillance State Is Primed for Criminalized Abortion,” by Lily May Newman, May, 2022. https://www.wired.com/story/surveillance-police-roe-v-wade-abortion/ last checked 7/8/2022.

The potential for misuse of this technology is enormous. It's not just the generic, philosophical concern about the intrusion on civil liberties. The concern is that it will be used for improper political purposes: to stifle dissent, monitor people with views that question the current authorities, etc. And the concern isn't really about any particular side of the political spectrum. It's about whomever might be in power. You know the old adage — power corrupts, absolute power corrupts absolutely. Unfortunately, both sides of the political aisle have that potential.

d. Some people are taking action

1. Private Groups

Now you can see what makes this issue so difficult. If put in the right hands, this technology could help society. But if it's abused, it could be quite harmful. For that reason I'd never argue that the use of this technology should be eliminated, but that it should be monitored and controlled. And there are plenty of groups trying to address the situation. Take, for instance,

> Nano, a 39-year-old developer, wants to make residents of Marseille more aware that they are being watched. She is part of a group called Technopolice that has been organizing efforts to map the rise of video surveillance. With some 1,600 cameras in the city, there is plenty to find. Mixed in among them, Nano says, are 50 smart cameras designed to detect and flag up suspicious behavior, though she is unsure where they are or how they are being used.[59]

2. Governments

It's become clear that there needs to be some larger restriction on this type of AI. Bernard Marr explained in Forbes:

> Governments, too, clearly understand that there is a need for a regulatory framework, as evidenced by the existence of the EU's proposed Artificial Intelligence Act. The proposed act prohibits authorities from using AI to create social scoring systems, as well as from using facial recognition tools in public places.[60]

---

[59] MIT Technology Review, "Marseille's battle against the surveillance state" by Fleur Macdonald, June 13, 2022, https://www.technologyreview.com/2022/06/13/1053650/marseille-fight-surveillance-state/ last checked 7/8/2022.

[60] https://www.forbes.com/sites/bernardmarr/2021/09/27/the-5-biggest-technology-trends-in-2022/?sh=4bafc07c2414, last checked 1/12/2022.

Various researchers have been raising their voices about the concerns with the technologies and it appears that, "governments are trying to make software more accountable."[61]

> Last December, the New York City Council passed a bill to set up a task force that will recommend how to publicly share information about algorithms and investigate them for bias. This year, France's president, Emmanuel Macron, has said that the country will make all algorithms used by its government open. And in guidance issued this month, the UK government called for those working with data in the public sector to be transparent and accountable. Europe's General Data Protection Regulation (GDPR), which came into force at the end of May, is also expected to promote algorithmic accountability.[62]

3. The Tech World

For their part, the AI world seems to be catching on. A recent article explained that, "Ethicists have long debated the impacts of AI and sought ways to use the technology for good, such as in health care. But researchers are now realizing that they need to embed ethics into the formulation of their research and understand the potential harms of algorithmic injustice…"[63]

4. Lawyers?

I believe there is a role for lawyers in this fight as well. And I think the ethics rules demand that we fill it.

> i. Lawyers have always had a responsibility to larger societal issues. Consider Pro Bono Work.

The lawyer's duty to help the poor has been long established. Actually, it's not just the "poor" because the category also includes the "disadvantaged" and the "underserved." What the issue is really about is helping people obtain access to justice. The category thus includes those people who have a barrier to access to justice and usually that barrier is a financial one. This obligation has been accepted in the practice for some time now.

---

[61] https://www.nature.com/articles/d41586-018-05469-3, last checked 6/20/2021.

[62] https://www.nature.com/articles/d41586-018-05469-3, last checked 6/20/2021.

[63] https://www.nature.com/articles/d41586-020-00160-y, last checked 6/19/2021.

We see a reference to this duty as far back as 1965 in the now outdated disciplinary rules, the Model Code of Professional Responsibility (that *Code* was eventually scrapped in its entirety and our existing disciplinary rules are based on the Model *Rules* of Professional Responsibility which were promulgated by the ABA in 1983). The Code stated, "As a society increases in size, sophistication and technology, the body of laws which is required to control that society also increases in size, scope and complexity. With this growth, the law directly affects more and more facets of individual behavior, creating an expanding need for legal services on the part of the individual members of the society."[64] In other words, as society advances, the obstacles to access to justice increase. That only enhances the need for lawyers to help the disadvantaged. Over the years, scholars have expanded upon that idea.

Professor Deborah L. Rhode (now of Stanford Law School) set forth a variety of justifications for the pro bono duty in an article she wrote back in 1999 in the Fordham Law Review. She explained that, "Lawyers have a monopoly on legal services, thus creating the duty to help provide them for the poor."[65] Additionally, lawyers are a key guardian of justice and for that reason we have the obligation to provide legal services for those who can't afford them. Professor Rhode pointed to a more practical justification as well: "the benefit that such work confers upon the lawyers themselves," which includes the, "intrinsic satisfactions that accompany public service."[66] She continued, "The primary rationale for pro bono contributions rests on two premises: first, that access to legal services is a fundamental need, and second, that lawyers have some responsibility to help make those services available. The first claim is

---

[64] See the Model Code footnote to EC 2-25, citing Comment, Providing Legal Services for the Middle Class in Civil Matters: The Problem, the Duty and a Solution, 26 U. PITT. L REV. 811, 811-12 (1965).

[65] Deborah L. Rhode, Cultures of Commitment: Pro Bono for Lawyers and Law Students, 67 Fordham L. Rev. 2415 (1999) at 2419.

[66] Deborah L. Rhode, Cultures of Commitment: Pro Bono for Lawyers and Law Students, 67 Fordham L. Rev. 2415 (1999) at 2420.

widely acknowledged."[67] Proof that it continues to be is widely acknowledged comes from the State of New York where recently Chief Judge Jonathan Lippman of the New York Court of Appeals acknowledged that "lawyers have a professional responsibility to promote greater access to justice."[68] He explained that, "as far back as judges and lawyers have existed, the pursuit of equal justice for all, rich and poor alike, has been the hallmark of our profession." And the responsibility doesn't stop with practicing attorneys. He continued, "each attorney has an obligation to foster the values of justice, equality, and the rule of law, and it is imperative that law students gain a recognition of this obligation as part of their legal training." [69]

The idea that lawyers should "give back" to society isn't so controversial. In fact, my gut tells me that the majority of people in the practice would agree with the need for lawyers to help the disadvantaged community. In theory, it seems to simply be an extension of our otherwise accepted societal wide notion of helping the needy.

ii. The Preamble as justification for lawyers taking action

Lawyers have a large role in society. We don't just owe a duty to our clients, rather the codes of professionalism in every state acknowledge that we also owe a duty to our communities and even society as a whole. That's why we champion things like Access to Justice, Diversity and Inclusion, and other similarly important ideals. It's because we know that our special role allows us to have an oversized impact in realizing those concepts. Plus, the privilege that we have to practice law demands that we take responsibility for making such

---

[67] Deborah L. Rhode, Cultures of Commitment: Pro Bono for Lawyers and Law Students, 67 Fordham L. Rev. 2415 (1999) at 2418.

[68] http://www.nycourts.gov/attorneys/probono/FAQsBarAdmission.pdf, last checked by the author on 12/27/2014.

[69] http://www.nycourts.gov/attorneys/probono/FAQsBarAdmission.pdf, last checked by the author on 12/27/2014.

important paradigms become a reality. I believe that the same obligation exists with AI powered facial recognition technology.

The ethics rules reflect the requirement for lawyers to pursue these larger goals. For instance, in the Preamble to the Rules, we find the following section:

> Preamble [1] A lawyer, as a member of the legal profession, is a representative of clients, an officer of the legal system and a public citizen having special responsibility for the quality of justice.

What does it mean to have a "special responsibility?" The very nature of the word "special" means that it's something out of the ordinary. When read in connection with the rest of the section, I believe that the special responsibility includes ensuring that the "quality of justice" is in step with societal advancements.

For instance, there was a time when our practice was made up of almost all white men. But as society advanced, we grew to appreciate the importance of diversity. In fact, the practice eventually made diversity a goal and today we have a significant emphasis on that — including, in some states, MCLE that's geared toward elimination of bias. That requirement is an example of how we took our "special responsibility for the quality of justice," made changes in the practice and brought about a desired change. Today we have an opportunity to do that again, in an even bigger way. And example of the latest evolution in thinking is the idea of "access to justice."

As I mentioned earlier, the idea of ensuring that more people have access to justice is not a new concept. What is new, however, is the emphasis. It's only been the past several years that you've heard people talking about this concept in a more vocal manner. In fact, we see a reference in the rules:

> Preamble [6] …A lawyer should be mindful of deficiencies in the administration of justice and of the fact that the poor, and sometimes persons who are not poor, cannot afford adequate legal assistance. Therefore, all lawyers should devote professional time and resources and use civic influence to ensure equal access to our system of justice for all those who because of economic or social barriers cannot afford or secure adequate

> legal counsel. A lawyer should aid the legal profession in pursuing these objectives and should help the bar regulate itself in the public interest.

If lawyers actually pursue the mandate of the rules— if we devote time and resources to ensure equal access to our justice system for all, then we could make wide reaching societal change. That change affects people beyond the practice because it's a society-wide effort. By reducing these obstacles to justice, lawyers have a real chance to save the world.

It makes me wonder — should lawyers be talking a larger role in monitoring artificial intelligence throughout society? I mean, beyond considering the disciplinary implications. I'm talking about a larger role throughout society. It seems that our ethics rules mandate that we take a larger role. Look at the Preamble again, except now consider the issue of AI:

> [1] A lawyer, as a member of the legal profession, is a representative of clients, an officer of the legal system and a public citizen having special responsibility for the quality of justice.
>
> [5] A lawyer's conduct should conform to the requirements of the law, both in professional service to clients and in the lawyer's business and personal affairs. A lawyer should use the law's procedures only for legitimate purposes and not to harass or intimidate others. A lawyer should demonstrate respect for the legal system and for those who serve it, including judges, other lawyers and public officials. While it is a lawyer's duty, when necessary, to challenge the rectitude of official action, it is also a lawyer's duty to uphold legal process.
>
> [6] As a public citizen, a lawyer should seek improvement of the law, access to the legal system, the administration of justice and the quality of service rendered by the legal profession. As a member of a learned profession, a lawyer should cultivate knowledge of the law beyond its use for clients, employ that knowledge in reform of the law and work to strengthen legal education.

It appears that AI powered surveillance like facial recognition technology is being used to take advantage of vulnerable people. When one combines the other dangerous uses of artificial intelligence, then very serious concern for society as a whole. Maybe it's time for lawyers to add this issue to the roster of societal issues that we, as a profession confront. The need to do so seems to stem quite clearly from the obligations set forth above from the Preamble.