Oregon State Bar CLE Seminars

ChatGPT, Legal Ethics, and Beyond



Wednesday, March 12, 2025, 9 a.m.–12:15 p.m.

3 Ethics (Oregon specific) credits

The materials and forms in this manual are published by the Oregon State Bar exclusively for the use of attorneys. Neither the Oregon State Bar nor the contributors make either express or implied warranties in regard to the use of the materials and/or forms. Each attorney must depend on his or her own knowledge of the law and expertise in the use or modification of these materials.

Copyright © 2025

OREGON STATE BAR
16037 SW Upper Boones Ferry Road
P.O. Box 231935
Tigard, OR 97281-1935

TABLE OF CONTENTS

Faculty v

ChatGPT, Siri, and Alexa Are Out to Get You! 1
1. The More Things Change, the More They Stay the Same. 1
2. Chatbots: The Legal Marketing Device That Could Get You in Trouble 17
3. Attorney Ethics in the Meta Verse 23
4. More Controversial Uses of AI Technology and the Role Lawyers Should(?) Play . . 26
5. Supervising Software? 37
6. Big Data 39
7. The Problem with the IoT 42
8. Five Ethical Ways Lawyers Can Use ChatGPT 44

NOTES

FACULTY



Stuart I. Teicher, Esq., is a professional legal educator who focuses on ethics law and writing instruction. A practicing lawyer for 30 years, Mr. Teicher's career is now dedicated to helping fellow lawyers survive the practice of law and thrive in the profession. Mr. Teicher teaches seminars, provides in-house training to law firms and legal departments, provides CLE instruction at law firm client events, and gives keynote speeches at conventions and association meetings. Mr. Teicher is a Supreme Court appointee to the New Jersey District Ethics Committee, where he investigates and prosecutes grievances filed against attorneys. Mr. Teicher is an adjunct professor of law at Georgetown Law, where he teaches Professional Responsibility.

NOTES

CLE Performer & Ethics Educator
stuart.teicher@iCloud.com
www.stuartteicher.com
732-522-0371
© 2024 Stuart Teicher, Esq.

Chat GPT, Siri, and Alexa are out to get you!
Program Written Materials

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."[1] From a more technical perspective, "cloud computing" encompasses several similar types of services under different names and brands, including: web-

[1] 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.

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."[2]

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 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).

These issues regarding Chat GPT and generative AI are elaborated in the recent opinion from the State of Florida and guidelines form the State of New Jersey. Those are both attached to these materials. And it doesn't matter if you're not barred in one of those states — they are great guides for us all because they address the general ethics issues that are relevant in all states.

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

[2] Pa Opinion 2011-200 at 1

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."[3]

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.[4] 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

---

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

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

advertising that reflects the keywords in the e-mail."[5] 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 transmit confidential information.[6] 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."[7]

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

---

[5] NYSBA Op. 820 at 2

[6] NYSBA Op. 820 at 1

[7] NYSBA Op, 820 at 2

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.[8]

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

---

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

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."[9]

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.[10] 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…"[11]

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

---

[9] 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.

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

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

is not a per se confidentiality violation.[12] The lawyer wasn't strictly liable for an ethics violation "even if an unauthorized or inadvertent disclosure should occur".[13] 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 safeguard confidential client information and communications from inadvertent and unauthorized disclosure."[14]

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.[15] 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."[16] 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

---

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

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

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

[15] 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

[16] NJ Opinion 701, at 3.

> 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 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."[17] 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

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

measures might become obsolete.[18] 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."[19] 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."[20]

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

[18] Arizona Opinion 09-04 at 2.

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

[20] Alabama Ethics Opinion 2010-02 at 16

communication with clients); see also N.Y. State 820 (2008) (addressing Web-based email services)."[21]

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 communication generally) should monitor these legal developments, especially regarding instances when using technology may waive an otherwise applicable privilege. *[citation omitted]*."[22]

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.

---

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

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

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 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")."[23]

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

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

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 June 28th, sheds even more light on the company's privacy practices with regard to its digital voice assistant.[24]

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

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

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 purposes of enforcing adherence to ethical standards is grounds for concluding that the lawyer has violated [the rule]."[25]

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.[26] 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."[27] 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

---

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

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

[27] Oregon Opinion 2005-141 at 386.

retains the obligation to ensure that appropriate standards concerning client confidentiality are maintained by the contractor."[28]

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 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."[29]

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:[30]

> "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.[31]

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* --

---

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

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

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

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

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 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. How Rule 1.18 Works

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. <u>Win the ethical battle, but lost the disqualification war</u>

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. How to make chatbots safer

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.[32]

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

[32] 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.[33]

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.[34]

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,

---

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

[34] 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,[35], biases in algorithms[36] and surveillance uses like facial recognition[37].

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.
>
> 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.[38]

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.

---

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

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

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

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

> 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

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."[39]

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:

> 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.[40]

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.

---

[39] 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.

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

> ‘We are very concerned about research which involves consent from vulnerable populations…’[41]

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 nationwide security law, adopted last year, allows for video surveillance by police drones during events like protests and marches.[42]

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,”[43] 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.[44]

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

---

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

[42] 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.

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

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

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.[45]

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 offer 'gun detection' algorithms."[46] 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."[47] 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."[48]

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.

---

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

[46] "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.

[47] "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.

[48] "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.

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."[49]

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

[49] "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.

> designed to detect and flag up suspicious behavior, though she is unsure where they are or how they are being used.[50]

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.[51]

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."[52]

> 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.[53]

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…"[54]

---

[50] 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.

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

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

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

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

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.

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."[55] 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

---

[55] 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).

duty to help provide them for the poor."[56] 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."[57] 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 widely acknowledged."[58] 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."[59] 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." [60]

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

---

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

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

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

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

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

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 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.

5. Supervising Software?

The future of AI in the practice will probably mirror the future we're seeing in other business categories. Specifically, we may see AI being used in "predictive coding."

> "Essentially, predictive coding is a process whereby a machine learns from watching human behavior and then applies what it learns. This is the technology behind how Amazon and Google seem to always know what you are looking for before you start looking. The machine's learning algorithms are designed to gather data, analyze it, and then make decisions about what is relevant. And because of the increased computing power on these machines, this is done very quickly."[61]

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

Think about it— if the machines watch human behavior, then apply what it learns, it could evaluate the probabilities of various outcomes and deliver valuable information that would assist a client in making strategic decisions. While that concept seems to foreshadow

[61] http://www.americanbar.org/publications/gp_solo/2014/may_june/how_technology_changing_practice_law.html, last checked by the author on 4/2/2017.

the elimination of attorneys, in a strange way I think it also reveals the reason lawyers will actually never vanish from the equation. Yes, the ability of AI to perform these types of tasks in an efficient manner means that there will very likely be a decrease in the number of support staff that lawyers require. There will also probably be a decrease in the need for the vast number of junior associates, since they perform a lot of the routine tasks that AI will now address. But while there will be a decrease in the number of lawyers that might be needed, there will always be a need for human counsel.

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

First, we must put an increased emphasis on supervising…our technology people. Remember, we may be replacing associates, but the software that replaces them does not run itself. There are always support personnel needed to make these things work. And those support personnel might not be located in your office- they might be some third party contractor or employees of the company that provides the software. Right now you should be thinking about Rule 5.3. Those support personnel would probably be considered the "nonlawyer assistance" that we are required to supervise per 5.3. And don't get fooled into thinking that you don't need to supervise them just because they are an independent consultant. As we've discussed in this program, the "nonlawyer assistance" category is expanding and a tech vendor who helps run our AI services is probably going to be covered by 5.3.

Second- and I know this is stretch, but I don't think it's so crazy… could we soon see an emerging duty to supervise the *technology*? The new Rule 5.3 refers to "nonlawyer assistance." Admittedly, the rule currently refers to the lawyer's need to "make reasonable efforts to ensure that the *person's* conduct is compatible with the professional obligations of

the lawyer…" Rule 5.3(b), emphasis added. In referring to those non lawyers, Rule 5.3, Comment [2] states,

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

As these systems get more complex, and as we start to eliminate staff and allow lawyers to utilize these systems directly, I can foresee these systems, themselves, being seen as virtual assistance that require supervision by the lawyer. I can see this comment being altered ever so gently to include the systems, in addition to humans.

Maybe I'm wrong. Maybe, instead, it will mean greater emphasis on supervising the programmers, developers, and the support personnel who create and implement these systems. But I wouldn't count it out. I see part of my job as looking into the future and predicting where our ethical duties are headed. I think that it's reality to consider that, in the future, super complex software will be considered nonlawyer assistance that will require the lawyer's direct supervision. Just my two cents. Oh, and maybe three cents….

…and let me tell you where I also think that expanded duty of supervision is heading….robots. Yes, I said robots…and I'm not joking But that's for another program.

6. Big Data

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

There are two aspects to the idea "Big Data" thatt will be covered in this section. The first is the concept of gathering and analyzing the data. The second is what's commonly

referred to as "The Internet of Things (abbreviated as IoT). Competence demands that we understand what these things are, so here are the definitions of both.

Big data is exactly what you'd think it is— the collection and analyzation of data. That includes purchase histories, locations, and information about literally everything else. After the data is collected it's analyzed to reveal patterns that can be used in various business, political, and other manners. In many instances the data is used to create predictive models.[62]

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

> Big Data works on the principle that the more you know about anything or any situation, the more reliably you can gain new insights and make predictions about what will happen in the future. By comparing more data points, relationships begin to emerge that were previously hidden, and these relationships enable us to learn and make smarter decisions. Most commonly, this is done through a process that involves building models, based on the data we can collect, and then running simulations, tweaking the value of data points each time and monitoring how it impacts our results. This process is automated – today's advanced analytics technology will run millions of these simulations, tweaking all the possible variables until it finds a pattern – or an insight – that helps solve the problem it is working on.
>
> Until relatively recently, data was limited to spreadsheets or databases – and it was all very ordered and neat. Anything that wasn't easily organised into rows and columns was simply too difficult to work with and was ignored. Now though, advances in storage and analytics mean that we can capture, store and work with many, many different types of data. As a result, "data" can now mean anything from databases to photos, videos, sound recordings, written text and sensor data.
>
> To make sense of all of this messy data, Big Data projects often use cutting-edge analytics involving artificial intelligence and machine learning. By teaching computers to identify what this data represents– through image recognition or natural language processing, for example - they can learn to spot patterns much more quickly and reliably than humans.[63]
>
> Harold H. Hines, Jr. professor of medicine and director of the Center for Outcomes Research and Evaluation at the Yale School of Medicine, likened big

---

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

[63] Bernard Marr, *What Is Big Data? A Super Simple Explanation for Everyone*, BERNARDMARR.COM, https://www.bernardmarr.com/default.asp?contentID=766 (last visited May 21, 2018).

> data to the microscope—a device that didn't do anything on its own but also enabled a new way of seeing. The microscope was a tool that enabled a process that produced germ theory. Krumholz's view of big data's ultimate potential is similar, "It will create immense opportunities." If we do our part to use big data effectively, Krumholz said, it could launch a "new age of discovery."[64]

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

> Simply put, this is the concept of basically connecting any device with an on and off switch to the Internet (and/or to each other). This includes everything from cellphones, coffee makers, washing machines, headphones, lamps, wearable devices and almost anything else you can think of. This also applies to components of machines, for example a jet engine of an airplane or the drill of an oil rig. As I mentioned, if it has an on and off switch then chances are it can be a part of the IoT. The analyst firm Gartner says that by 2020 there will be over 26 billion connected devices... That's a lot of connections (some even estimate this number to be much higher, over 100 billion). The IoT is a giant network of connected "things" (which also includes people). The relationship will be between people-people, people-things, and things-things.[65]

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

Big data can be used in the practice of law in a variety of ways. It could be useful in analyzing transactions to determine the probability that a deal will close, or whether a litigant will be successful in litigation. There are lots of articles on the way big data could be valuable in the substantive practice of law, but that's not the focus of this section. Here we'll address the ethical issues that lawyers face. But first, let's get one confusing item out of the way. Lawyers hold a lot of information— does that make us "big data?"

Lawyers are not the same as the generic big data collectors. Yes, we hold client information, so to that extent, we are data collectors of sorts. But we don't have the same

---

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

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

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

7. The Problem with the IoT

1. What is frictionless computing?

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

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

> Amazon's Echo speaker, which uses Alexa, and Snap Inc.'s new Spectacles, camera-bearing sunglasses, are examples of what Benedict Evans, partner at venture-capital firm Andreessen Horowitz, calls "frictionless computing"—easy-to-use devices that unite applications with hardware beyond smartphones. Ben Schachter, senior analyst at Macquarie Capital, says: "Our view is the next big innovation will be from outside the device—from the software." He expects increasing use of such software to meet entertainment, health-care, home innovation and automotive needs.[66]

The words in that quote that should give lawyers pause are "outside the device." That's because the increased use of cell phones to connect with external hardware by way of an installed app increases the likelihood that hackers can get access to devices. A similar

---

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

concern surfaced quite recently in the medical community, with the vulnerability of heart devices to hacking:

> On Monday, the U.S. Food and Drug Administration published a public safety notice confirming it is possible for a hacker to remotely compromise security in St. Jude's wireless communication network and then secretly change commands in a pacemaker or implantable defibrillator while it's still wired to a patient's heart . . . ."As medical devices become increasingly interconnected via the internet, hospital networks, other medical devices and smartphones, there is an increased risk of exploitation of cybersecurity vulnerabilities, some of which could affect how a medical device operates," the FDA's Monday safety alert says.[67]

2. Hacking

While that isn't frictionless computing when using a cell phone, it is an external device controlled by computers via wireless communication. In that regard, it is an analogous problem. And that problem is clear: once there is increased use of that type of wireless communication between devices, the chances rise that hackers can wreak havoc. Although many of these opportunities to exploit devices have existed for a while, the concern is the increased chance of compromising data. As the use of this technology grows, there are increased opportunities for phishing, wireless hacking, etc. Thus, as frictionless computing becomes more prevalent, it greatly increases the opportunity for the hackers to get individuals' private information.

Personally, I'm willing to take the risk. I like using these devices, I understand the potential hacking problem, and I am willing to accept the downside in order to make use of this new technology. I am willing to put my personal information at risk. I am not, however, willing to put my client's information at risk.

Many lawyers use their personal devices to access work information. They like to have remote access to notes apps like Evernote and cloud storage sites like DropBox. Lawyers text clients and receive work emails, and that's all sent to and from personal devices. It's that same

---

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

device that will be used to engage further in frictionless computing— many lawyers are probably Alexa addicts already, for instance. To date, lawyers feel comfortable mixing business and personal use because they put password protections on the device and take other reasonable measures to protect client information. But at some point, vulnerabilities will increase to such an extent that the definition of what constitutes "reasonable measures" will change. The increased use of frictionless computing is likely hastening that change.

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

Bear in mind that this isn't about eliminating risk. Risk can never be completely eliminated. The central question is, "when does the risk expand to a point where it's necessary to take some different action?" As usual, there is no way to discern exactly when that line is crossed. But it's my job to tell you when the warning signs appear. Well . . . boom, they appeared. Keep your eyes open and make the move when you think it's warranted. Just don't get blindsided.

8. Five Ethical Ways Lawyers Can Use Chat GPT

Generative AI (gAI) offers numerous opportunities for enhancing legal practice efficiency and effectiveness. However, lawyers must ensure that their use of AI tools aligns with the Rules of Professional Conduct. Here are five ways lawyers can leverage generative AI while remaining compliant with the ethics rules.

Before we get to the different uses, let's talk about a preliminary ethics reality. Here's what I've learned after using Generative AI extensively in my work. Generative AI will only be safe for people who have a high level understanding of the area of law they are practicing. That's because of the hallucinations.

Generative AI makes mistakes. We all know that, and the purpose of this program is not to explain why or how. I'm assuming we all understand that already, and we accept it. We also know that the companies developing gAI are touting the low number of mistakes their systems make. I'm sure that the instances of hallucinations will be decreasing with each successive advancement of the technology.

But I don't think that matters for some people. I believe that one should not be using gAI for substantive matters unless one has a higher-than-minimum level of competence in the area of law one practices. Here's why.

Think about going to the dentist. Let's say you needed a crown. In the past, dentists would take physical impressions of people's mouths. They'd use yucky dental material that would go into a tray, they'd stick the tray into your mouth, you'd bit down on it, and your physical bite would leave an impression on that dental material. The material hardens, they take the tray out of your mouth, and they'd send that impression to the lab. The lab would use that physical impression to make a crown that matched your existing tooth and that's what the dentist would place in your mouth. These days, they don't use that gook any more.
Now the dentist uses a digital scanner. They put a wand into your mouth that has an optical sensor on it, and that sensor takes a scan of your mouth. The scan goes into the computer, the scan is then sent to the lab, and the lab uses that to make the tooth that they send to the dentist to insert into your mouth. The problem is, sometimes the digital scanner makes mistakes.

Sometimes the scanner incorrectly captures things, or it doesn't articulate things correctly, that sort of thing. A seasoned dentist who has experience in that work will be able to look in the patient's mouth and see that the scan is not accurate. An inexperienced dentist will

not. The inexperienced dentist will think that it looks ok, but they won't realize they are missing the error. The scan will be sent to the lab, and when the tooth comes back it won't fit.
It's the same thing with lawyers and Chat GPT. Generative AI is an outstanding tool that can do amazing things. But it has limitations and flaws and it sometimes gives bad results. And when it hallucinates, often times it does so very convincingly. It can fool a novice lawyer. Other times the mistakes is makes are so nuanced that someone other than a seasoned practitioner won't catch it.

That doesn't mean we shouldn't use it in the practice. It means that bad lawyers shouldn't be using it. It means that lawyers who have just the bare minimum competence shouldn't use it…unless they check absolutely everything or collaborate with someone with greater expertise.

A. Legal Research and Document Review

Okay, so this one is the toughest, so we might as well address it first. Despite the famous Avianca case (which we all know, so there's no reason to talk about it again), it is possible to use gAI for legal research. You've just got to be super careful.
Using generative AI for legal research and document review can save time and increase accuracy. Rule 1.1 on Competence requires lawyers to provide competent representation, which includes staying informed about the benefits and risks associated with technology (Comment 8).

> Rule 1.1. Competence.
> A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.
>
> [8] Maintaining competence. — To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.

By using AI tools for research, lawyers can efficiently access and analyze vast amounts of legal information, ensuring they meet the standard of competence.

Also, remember that anything you put into these publicly available gAI systems like Chat GPT will be used as training data and could be spit out in response to other people's queries in the future. Confidentiality, therefore, mandates that we don't put client information into our queries. Plus, remember not to give too many details, or that might also run afoul of Comment [4] to Rule 1.6:

> Rule 1.6, Comment [4]
> Paragraph (a) prohibits a lawyer from revealing information relating to the representation of a client. This prohibition also applies to disclosures by a lawyer that do not in themselves reveal protected information but could reasonably lead to the discovery of such information by a third person. A lawyer's use of a hypothetical to discuss issues relating to the representation is permissible so long as there is no reasonable likelihood that the listener will be able to ascertain the identity of the client or the situation involved.

B. Drafting Legal Documents

Generative AI can assist in drafting various legal documents, from contracts to pleadings. But you need to make sure that the work being done by the system is correct. That's about supervision.

Rule 5.3 on Responsibilities Regarding Nonlawyer Assistance emphasizes that lawyers must ensure that their use of nonlawyer services, including technology, is compatible with their professional obligations.

> Rule 5.3. Responsibilities regarding non-lawyer assistance.
>
> With respect to a nonlawyer employed or retained by or associated with a lawyer:
>
> (a) a partner in a law firm, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm, shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that the person's conduct is compatible with the professional obligations of the lawyer;
>
> (b) a lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer; and

(c) a lawyer shall be responsible for conduct of such a person that would be a violation of the Rules of Professional Conduct if engaged in by a lawyer if:

(1) the lawyer orders or, with the knowledge of the specific conduct, ratifies the conduct involved; or
(2) the lawyer is a partner or has comparable managerial authority in the law firm in which the person is employed, or has direct supervisory authority over the person, and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.

Here is where this duty is heading. In the not too distant future, gAI is going to be considered "nonlawyer" assistance that needs to be supervised. The duty of supervision will be extended to a duty to supervise our software.

The reality is that lawyers must supervise and verify AI-generated documents to ensure accuracy and compliance with legal standards, maintaining responsibility for the final output. And don't be afraid to get some help if you're not sure about the accuracy of the substantive parts of the documents these systems create. Rule 1.1 allows you (but does not require) collaborating with other lawyers (bullet points added by me):

Rule 1.1, Comment [1] Legal knowledge and skill. — In determining whether a lawyer employs the requisite knowledge and skill in a particular matter, relevant factors include
- the relative complexity and specialized nature of the matter,
- the lawyer's general experience, the lawyer's training and experience in the field in question,
- the preparation and study the lawyer is able to give the matter and
- whether it is feasible to refer the matter to, or associate or consult with, a lawyer of established competence in the field in question.

In many instances, the required proficiency is that of a general practitioner. Expertise in a particular field of law may be required in some circumstances.

C. Advice, Predictive Analytics and Case Strategy

a. Assisting in giving advice

Generative AI can analyze past case outcomes to provide insights and predictions about the likely success of various legal strategies. Rule 2.1 on Advisor emphasizes that lawyers should provide candid advice, considering both legal and non-legal factors. By using AI to inform their strategies, lawyers can offer well-rounded advice based on comprehensive data analysis while ensuring they interpret and present AI findings accurately. Look at this example of how it could be helpful in this regard.

I wanted to focus on the second part of Rule 2.1. The second sentence says that lawyers are permitted to consider a variety of issues when giving advice, including moral issues. So I asked Chat GPT, “What are the moral implications of selling a business that isn't performing up to one's profit expectations for more than it might be worth?” Here’s it’s response:

> Selling a business that isn't meeting profit expectations for more than its actual worth raises several moral implications:
>
> 1. Honesty and Transparency
> · Moral Obligation: Sellers have a duty to be honest about the business's financial health and performance. If the seller knowingly conceals poor profitability or exaggerates the potential of the business to inflate its price, this can be seen as deceptive.
> · Buyer’s Expectations: Misleading buyers into believing the business is worth more than it actually is could result in financial harm to the buyer, violating principles of fairness and trust.
>
> 2. Buyer’s Due Diligence
> · Moral Gray Area: While sellers have a responsibility to be transparent, buyers are also expected to conduct thorough due diligence. If a buyer fails to investigate the business’s true value, some might argue that the responsibility partly falls on the buyer. However, this doesn’t absolve the seller from the responsibility of providing accurate information.
>
> 3. Fair Market Value
> · Fairness: The fair market value of a business is what a willing buyer is ready to pay, and the worth of a business can be subjective. However, if the seller inflates the price based on inaccurate or incomplete information, this distorts the fairness of the transaction.
> · Ethical Pricing: Selling at a price that reflects the true state of the business, including any challenges or underperformance, respects the ethical principle of fairness.
>
> 4. Long-Term Consequences
> · Reputation: Misrepresenting a business’s value may damage the seller’s reputation within the industry and among peers, which can have long-term professional and personal consequences.
> · Legal Risks: While this question focuses on moral implications, there may also be legal considerations. Misrepresenting the value of a business in a sale could result in fraud claims or lawsuits.
>
> 5. Moral Theories
> · Utilitarianism: From a utilitarian perspective, inflating the price may harm the buyer while temporarily benefiting the seller. The overall harm (to the buyer, employees, and stakeholders) would outweigh the benefit (profit for the seller), making it unethical.
> · Kantian Ethics: Kantian ethics focuses on the idea of treating others as ends in themselves, not as means to an end. If a seller misleads a buyer to maximize profit, they are treating the buyer merely as a means to their financial gain, which is morally wrong according to Kantian principles.

In short, selling a business for more than it might be worth, especially through misrepresentation or withholding key information, raises significant moral concerns around fairness, honesty, and integrity.

b. Predictive Analytics and Case Strategy

Chat GPT can also help formulate a strategic plan for pretty any matter. I asked it, "What are the chances of me beating a ticket in New Jersey for a violation of N.J.S.A 39:4-97 if I hit someone from behind." It gave me the following response:

In New Jersey, N.J.S.A. 39:4-97 refers to careless driving, which is defined as driving without due caution in a way that endangers or is likely to endanger people or property. If you rear-ended another vehicle, you're generally presumed to be at fault, as drivers are expected to maintain a safe distance to avoid collisions. However, your chances of successfully contesting the ticket depend on several factors:
Factors That Affect Your Chances:
1. Proving You Weren't Careless
o Rear-end collisions often lead to an assumption of fault, but if you can demonstrate that you were not driving carelessly (e.g., the driver in front stopped suddenly for no reason, mechanical failure in your vehicle), this might help your defense.
o If road conditions were poor (e.g., ice, rain), you may argue that your actions were reasonable given the circumstances.
2. Contributory Negligence
o If the driver in front of you did something unexpected or illegal (e.g., suddenly cutting you off or braking without reason), you may argue that they contributed to or caused the accident, which could reduce or eliminate your liability.
3. Lack of Evidence
o The police officer issuing the ticket must establish that your driving was careless. If there's insufficient evidence (e.g., no witnesses or clear proof of carelessness), you might challenge the basis for the ticket.
4. Plea Bargain or Lesser Charge
o Even if you are technically at fault, you might be able to negotiate the charge down. For example, New Jersey offers a lesser charge of unsafe driving (N.J.S.A. 39:4-97.2), which doesn't carry points on your license, though it does involve higher fines.
5. Hiring an Attorney
o If the consequences of the ticket are significant (e.g., higher insurance premiums, points on your license), hiring an attorney can improve your chances of either beating the ticket or negotiating a more favorable outcome.

Possible Defenses:
· Sudden Emergency: If you were confronted with an unavoidable situation (like a car ahead of you stopping unexpectedly), you could argue that you acted reasonably under the circumstances.
· Mechanical Failure: If your car experienced a sudden brake failure or another mechanical issue that contributed to the accident, this could be a valid defense.
· Faulty Traffic Signal: If a malfunctioning traffic signal or other road conditions caused the accident, that might mitigate your responsibility.
Likelihood of Success

· Challenging fault in rear-end collisions is difficult but not impossible. Without strong evidence to show you weren't driving carelessly or that the other driver was at fault, your chances of beating the ticket may be low. However, negotiating the ticket down or reducing the penalties is more achievable.
Would you like more details on strategies to handle this situation in court?

I see this use as a double edged sword. It involves the ethical rules on Competence and Diligence.

Rule 1.1. Competence.

A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness, and preparation reasonably necessary for the representation.

Rule 1.3. Diligence.

A lawyer shall act with reasonable diligence and promptness in representing a client.

Yes, using Chat GPT to formulate a strategy can help us comply with our duty to be competent and diligent. But I think, in the near future, people are going to start to make the argument that consulting Chat GPT on strategic issues is required. I could imagine a malpractice action occurring and the plaintiff's lawyer runs the client's issue through ChatGPT. The system gives an idea that the lawyer being sued didn't think of. Or maybe it flags the issue the lawyer missed. The plaintiff's lawyer then claims that a reasonable lawyer would have consulted ChatGPT because they would have then noticed "XYZ."

4. Conflict Checking

AI can streamline conflict checking by rapidly cross-referencing client information and identifying potential conflicts of interest. I asked the system how it could help a lawyer in that regard. The answer it gave me what pretty good:

I can assist with conflict checking for lawyers by streamlining the process of identifying potential conflicts of interest. Here's how I can help:

1. Data Organization: I can help you organize client information, including names of parties, witnesses, and opposing counsel. This information can be categorized and stored systematically for easy reference during conflict checks.
2. Conflict Analysis: I can assist in analyzing cases or relationships to flag potential conflicts based on common criteria such as:

- Current or former client relationships
- Adverse interests between parties
- Confidentiality concerns

3. Keyword Search: I can quickly search through your existing records for any names or parties involved in a new case to identify overlaps, ensuring no conflicts arise based on previous work.
4. Summarizing Ethical Rules: I can provide summaries of relevant ethical rules (such as the ABA Model Rules of Professional Conduct or local bar guidelines) to guide you in determining whether a potential conflict exists and how it should be handled.
5. Decision Support: Based on the identified relationships and potential issues, I can assist in drafting waivers, consent forms, or other documents required to resolve conflicts.
6. Tracking and Reporting: I can help set up a system to track ongoing potential conflicts and ensure that all new cases are checked against past and current clients.

Then it asked me if I wanted a step-by-step outline for setting up an efficient conflict checking process. I said, "yes" and this is what I got. It's a pretty good guide for lawyers!

1. Data Collection and Organization

Start by gathering essential client data that will form the basis of your conflict check system:

- Current Clients: List active clients and matters.
- Former Clients: Include a record of all former clients with details of the matters you handled.
- Adverse Parties: Track opposing parties in each case.
- Associated Third Parties: Include witnesses, experts, co-counsel, or other involved parties.
- Key Personnel: If applicable, maintain details about employees or stakeholders in corporate clients.

This data can be organized into a spreadsheet or conflict check software, with fields for:

- Client/Party Name
- Matter Description
- Date of Representation
- Status (Current, Former)
- Opposing Counsel
- Other relevant details

2. Conflict Search System

To automate or streamline the process, use the following:

- Keyword Search: I can help you set up an easy keyword search system where you input a new client's details (e.g., names of the client and related parties). You would search these keywords against the database of current and past clients to identify any overlaps.

Example Tools: Excel with search/filter capabilities, conflict check software (e.g., Clio, Smokeball), or even document management systems.

- Confidentiality Flags: Tag certain cases or clients with confidentiality flags to ensure that even internal team members are aware of restrictions on sharing information.

3. Conflict Criteria Analysis

When a potential conflict is flagged, the next step is to analyze whether it constitutes a significant ethical issue:

· Same/Related Matter: Is the new matter related to a previous case where you represented the adverse party?
· Substantially Related Issues: Are there similar legal issues or facts?
· Duties of Loyalty and Confidentiality: Could the new representation violate duties to a former or current client?

4. Ethical Rule Summaries

You should be familiar with these key rules:
· ABA Model Rule 1.7 (Current Clients): Prohibits representation of conflicting interests without informed consent.
· ABA Model Rule 1.9 (Former Clients): Prohibits representation adverse to a former client in the same or substantially related matter without consent.
· Local Jurisdiction Rules: These often mirror ABA rules but might have nuances (e.g., state bar rules). I can draft quick summaries of these rules to guide your decision-making process in borderline cases.

5. Waiver and Consent Forms

If you identify a conflict, you may need to get consent from the affected parties. I can assist in drafting:
· Conflict Waiver Forms: Outlining the conflict and obtaining informed consent from both parties.
· Joint Representation Agreements: If you represent multiple clients in related matters, this agreement outlines potential conflicts and consent to proceed.

6. Ongoing Conflict Tracking

To ensure compliance over time, I can help you:
· Monitor Conflicts: Implement a system for checking ongoing cases regularly for potential new conflicts.
· Automate Reminders: Set up reminders to review conflict checks before taking on new clients.

7. Reporting and Compliance

Lastly, I can assist in setting up reports to ensure compliance with conflict check protocols, including:
· Periodic Reviews: Quarterly or bi-annual audits of conflict check logs.
· Documentation: Keeping clear records of conflict checks and any waivers signed.

NOTES