STUART I. TEICHER ESQ.

ETHICS EDUCATOR & CLE PERFORMER
stuart.teicher@icloud.com
www.stuartteicher.com
732-522-0371
@2018 Stuart Teicher, Esq.

The Cyborgs are Coming! The Cyborgs are Coming!
Program Written Materials

1. Introduction

The use of technology in the practice of law grows exponentially every day. An unfortunate outgrowth of that reality is that lawyers are being seen as an ever-increasing target of bad guys as well. It makes sense, then, that as the use and danger increases, the number of new ethics opinions on the topic increases as well. I've given a bunch of programs on the topic, but with each passing day there emerge new issues to explore. That's what we'll do in this program. Let's review the latest developments in the rules and explain a few new advisory opinions from across the country that govern a lawyer's use of technology in the practice. In the process we'll review some of the biggest tech-related disruptors to affect the practice of law today.

2. Overlapping ethics duties…which are broadening

The trend throughout the ethics world in a variety of contexts is that our ethical duties are broadening. That's particularly true in the world of technology ad social media. Here are a few duties that are broadening big time:

a. Competence:

Understanding the latest technology is required in order for a lawyer to maintain their minimum level of competence. That mandate is found in the rules, and it's also been reinforced in state ethics opinions.

In California, Rule 3-110 states:

> Failing to Act Competently
>
> (A) A member shall not intentionally, recklessly, or repeatedly fail to perform legal services with competence.
>
> (B) For purposes of this rule, "competence" in any legal service shall mean to apply the 1) diligence, 2) learning and skill, and 3) mental, emotional, and physical ability reasonably necessary for the performance of such service.
>
> (C) If a member does not have sufficient learning and skill when the legal service is undertaken, the member may nonetheless perform such services competently by 1) associating with or, where appropriate, professionally consulting another lawyer reasonably believed to be competent, or 2) by acquiring sufficient learning and skill before performance is required.

In ABA jurisdictions, Rule 1.1, Competence, states:

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

In addition, Comment [8] to Rule 1.1 reminds us that, "To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology…" Finally, a variety of state advisory opinions from the last several years have made it clear that lawyers have a duty to understand technology. In fact, it's so widely established that I'm not going to bother providing you with any one of the myriad of opinions from states across the country which confirm that fact. At this point it should be considered common knowledge. But there's more—recent opinions have confirmed that a lawyer's duty of competence regarding technology is not static, rather it is a changing responsibility.

A lawyer's duty of competence is broadening. Sure, we've always been responsible for understanding the law. But when it comes to technology, the recent changes to the rule and advisory opinions have made it clear that we are all responsible for understanding the *underlying technology*. That means we need to have a competence with the substantive technology itself. This was made apparent in an opinion out of California

In The State Bar of California's, Standing Committee on Professional Responsibility and Conduct, Formal Opinion No. 2015-193, the Bar faced a situation where a lawyer had only a basic knowledge of e-discovery. That surface knowledge ended up getting him in trouble and caused harm to the client (for reasons that we won't go into here).

The Bar explained that the lawyer should have had a better understanding of e—discovery. Specifically, they stated that, "An attorney's obligations under the ethical duty of competence evolve as new technologies develop and become integrated with the practice of law." Cal. Op. 2015-193. Did you get that? our duty evolves as new technologies become more prevalent in the practice.

In addition, the Bar stated that, "Attorney competence related to litigation generally requires, among other things, and at a minimum, a basic understanding of, and facility with, issues relating to e-discovery, including the discovery of electronically stored information ("ESI")." You could substitute any technology area in there— texting, social media, whatever. It's our responsibility to understand these things. And the key difference is that they are saying that we need to expand our understanding of the underlying technology, not jus the law about that technology. This is a broadening of our duty of competence.

b. Supervision:

Also from Opinion 2015-193…

> "The duty of competence …includes the duty to supervise the work of subordinate attorneys and non-attorney employees or agents. This duty to supervise can extend to outside vendors or contractors, and even to the client itself."

Did you get that? Our duty to supervise isn't just about supervising the people in our office anymore. According to this opinion, we need to make sure that we supervise people whom we might have considered independent contractors in the past. Plus we might have to supervise the client— not "guide" the client. Supervise the client itself. This is a major expansion to our obligations.

c. Broadening of the definitions regarding communication

It's not just our duties that are broadening. There are other parts of the code that indicate an expansion of our professional responsibilities. Consider how there are some "definitions" that are changing…

My children don't always use actual sentences when they speak with me. Occasionally I get a "sure" or "whatever." More often than not, however, it's a series of audible grunts. Over the years I've been able to decipher these noises and I've come to realize that they are primitive, albeit valid attempts at communication. That's what passes for communication at the teenage years. Grunts, moans, maybe even a raised eyebrow. When your kids are that age, you've got to expand what you'll accept as a communication or you might not interact with them at all. Just as a parent needs to broaden their view of what constitutes a communication, so too does a lawyer. A variety of sources confirm that the definition of what constitutes a "statement" or a "communication" that would trigger the rules is expanding. Consider the following case.

In 2016 a Missouri woman was indicted for suspected support of Islamic State. According to the Wall Street Journal, Safina Roe Yassi, "called for the killing of U.S. law enforcement employees and military members by retweeting posts that contained their detailed

personal information…According to the indictment, one of the tweets she retweeted contained the line, Wanted to kill. According to the government, this retweet and other social media postings by Ms. Yassin signaled her active support for ISIS and her intention to communicate threats on their behalf."[1]

The journal went on to report,

> "A novel issue is how the law should treat retweets, a feature that allows Twitter users to repost other people's tweets. In a court filing last month, Ms. Yassin's lawyer…said his client was 'merely reporting someone else's statements."

Here's why I think this is important. It's the first case I've seen where a prosecuting agency is trying to affix liability on a person as a result of something they shared on social media. It's the first case I've seen where the prosecution is claiming that by redistributing the content, the retweeter is primarily responsible for the statement as if they said it themselves.

This isn't the first time someone is getting in trouble because of something they're posting on the internet— there are lots of cases where people face liability for making some comment on social media. but I don't recall any other criminal matter where the defendant was being charged with being primarily liable for distributing another person's content. Here, the defendant redistributed someone else's statement, and the re-distributor is, therefore, being considered to have uttered the offending statement.

Ultimately, this case may fail. There are substantive criminal law issues, as well as first amendment concerns. But I'm not bringing this up because of the substance of this indictment. Rather, this case is about the expanding definition of a person's "statement" or a "communication."

If a prosecutor on the criminal world is taking this position, then it's only a matter of time before a prosecutor in an ethics context takes the position. I can envision some ethics investigator saying that a lawyer's retweet of someone's statement constitutes that lawyers

---

[1] Wall Street Journal, Saturday/Sunday, August 13-14, 2016, page A3.

statement, or "communication" under the rules. The attorney ethics implications are significant.

Consider the following hypothetical:

> You're representing a client in a particularly nasty land use application. The client wants to demolish an historic home and the local land use board is opposed to it. There is a lot of hostility between your client and the land use board because the board wants to save the structure. In an effort to put pressure on the board, your client fabricates the following statement and tweets it one evening, "East Bumble board turned down my application for a demolition permit. I don't care-starting construction tomorrow! Firing up the bulldozer!" You retweet that statement.[2]
>
> You know the statement isn't true because you were at the meeting earlier in the day where the board tabled the application without denying it. You also know that your client is overseas and has no intention of actually starting construction. He told you a few hours ago that he was going to take to Twitter just to "rattle the board's cage a little."
>
> However….one of the land use board members follows you on Twitter and sees the retweet. He believes that your client might actually take the action described and, to avoid the destruction of a potentially irreplaceable historic structure, he directs the board attorney to immediately file for an injunction against your client, which she does. The board incurs a significant cost.
>
> Could this be a misrepresentation that's actionable under the rule? Consider that Rule 4.1 states (in part), "In the course of representing a client a lawyer shall not knowingly: (a) make a false statement of material fact or law to a third person…" Does this statement qualify?

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

---

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

The obvious question is whether you can be said to have made the statement. In a world where a retweet constitutes a person's statement, then yes, you could be deemed to have made that false statement.

This issue would also arise any time a lawyer might make a "communication" as well. Rule 7.2(a), states that, "a lawyer may advertise services through…electronic communication…" If your partner posts on Facebook a statement saying "I am ready to accept new clients. Call me now for a free consultation!" If you share that, then you might be responsible for making the electronic communication. That might not be a problem, unless one day you share something that is not true, and you violate Rule 7.1.

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

d. The duty to periodically review our technological presence

The idea that lawyers should review their social media presence is common sense. But the ethical mandate to do so has only recently been developed. There are a variety of reasons why we should review our social media profiles. I think they are obvious, but here are two angles you might not have considered:

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

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

ii. Someone else might post something that violates the rule.

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

Several states have come forward with opinions mandating that lawyers check their profiles. In Formal Opinion 748, the New York County Lawyers Association Professional Ethics Committee opined in March 10, 2015 that, "New York lawyers should periodically monitor and review the content of their LinkedIn profiles for accuracy."

For a while that NY opinion was one of the only voices chiming in on the matter. However, the DC Bar recently gave us Ethics Opinion 370, entitled, "Social Media I: Marketing and Personal Use" where they said,

> "An attorney must monitor his or her own social networking websites, verify the accuracy of information posted by others on the site, and correct or remove inaccurate information displayed on their social media page(s). As set forth in comment [1] to Rule 7.1, client reviews that may be contained on social media posts or webpages must be reviewed for compliance with Rule 7.1(a) to ensure that they do not create the 'unjustified expectation that similar results can be obtained for others.'" (footnote omitted) DC Op. 370 at 3.
>
> "It is suggested that lawyers, particularly those who do not frequently monitor their social media pages, those who may not know everyone in their networks well, or those who wish to have an added layer of protection, utilize these heightened privacy settings. Aside from the potential ethical issues discussed herein, there are many good reasons for a lawyer to want to maintain a higher level of control over what content others may place on a lawyer's social media page(s)." DC Op. 370 at 3.

3. Ethics Issues with Big Data: The concerns with the LinkedIn/Microsoft Merger:

It was recently announced that Microsoft is buying LinkedIn. There are some hidden attorney-ethics implications about which we all need to be aware.

A review of the recent news articles announcing the acquisition reveals that a key motivating factor in Microsoft's purchase of LinkedIn was access to LinkedIn's data. Of course, sharing data is nothing new. But when companies improve their ability to share our data across various platforms, my ears perk up. Not just because it's creepy or because of obvious privacy implications. The type of data sharing they're contemplating in the Microsoft/LinkedIn combination makes me worry about confidentiality (and other) issues.

Why are they merging? According to the Wall Street Journal, Microsoft sees a critical synergy with LinkedIn. http://www.wsj.com/articles/microsoft-gains-link-to-a-network-1465922927.

> "LinkedIn's users are, arguably, Microsoft's core demographic. They also offer Microsoft something it has long sought but never had—a network with which users identify. Microsoft needs to persuade LinkedIn users to adopt that identity, and use it across as many Microsoft products as possible.
> Access to those users, as well as the enormous amounts of data they throw off, could yield insights and products within Microsoft that allow it to monetize its investment in LinkedIn in ways that the professional networking site might not be able to. [Microsoft CEO] Mr. Nadella already has mentioned a few of these, including going into a sales meeting armed with the bios of participants, and getting a feed of potential experts from LinkedIn whenever Office notices you're working on a relevant task."

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

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

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

There's a basic issue to be concerned about— Confidentiality. If Microsoft scours our Word documents and emails, then there could be Rule 1.6 confidentiality issues. That's so obvious that we don't need to spend time talking about it now. I think the more unusual issues come from the Calendar function…if they leverage the data in our Calendar, it could reveal our client relationships:

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

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

—If they leverage data in our Calendar, it could reveal key substantive information that could harm the client:

If Microsoft looks at our Calendar they can see that we're heading to a particular locale. They might then cross reference our LinkedIn connections and send a message to one of them

that says something like, “Your connection Bruce Kramer is going to Chicago next week. Why don't you look him up?"

That heads-up might give someone the incentive to look into our movements a bit more…and who knows what they could find. What if that if that info was given to a real estate agent that we know in Chicago…and maybe we are representing a successful land owner…and we’re clandestinely scouting a real estate purchase and we don’t want people to find out because if they figure out that we’re their on behalf of our deep-pocketed client, the purchaser will run up the price. That LinkedIn message that tipped off the real estate agent could cost out client a lot of money.

—If they leverage data in our Calendar, it could end up revealing a misrepresentation:

Imagine that Client A asks you to accompany them to a meeting in Los Angeles. You tell her that you can't go because you'll be on vacation on the East Coast. That's not true, however. The truth is that you’ve already scheduled a meeting with a potentially new client in Los Angeles. You didn't want Client A to know that you’d be in town because you didn't want to have to shuffle between clients- it would just be too much work. You could have told Client A that you'd be in town but you didn't have time to meet her, but you thought she’d be insulted. It was just easier to say you're far away and be done with it.

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

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

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

These are just a few issues. Some of these are clear ethics concerns, others are more akin to PR nightmares. Are they so terrible that we all need to get off LinkedIn right away? That might be a bit premature. After all, they only just announced the merging of the platforms- they haven't actually done anything yet. I don't know what dangers will actually be realized, or whether any dangers will be realized at all. What I do know, is that part of being a responsible attorney in this technological age is to be diligent in thinking about these issues. As lawyers practicing an ever-changing technological environment, we need to be aware of the potential problems. Keep your eye on the news and stay abreast about the detail regarding the integration of these two platforms. Then, if you determine that you need to act, do so. That way we are "keep[ing] abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology." Comment [8], Rule 1.1

4. The Frictionless Computing Concern

The next ethical landmine for lawyers is located in our cell phones. Specifically, I think we are very close to the point where lawyers need to have two devices— one for work, and one for our personal use. Here's why.

The Wall Street Journal recently reported that cell phone sales growth has stagnated. After years of incredible growth in sales, the pace of that growth has subsided significantly. The

new frontier, the article claims, 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.[3]

The words that scare me in that quote 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 our devices. Just this week we saw a similar concern from the medical community. The Minneapolis Star Tribune reported about the vulnerability of hacking heart devices:

> 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.[4]

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 we start to increase the use of that type of wireless communication between devices, we increase the chance that hackers can wreak havoc. Yes, many of these opportunities to exploit our devices have existed for a while, but the concern I

---

[3] http://www.wsj.com/articles/the-next-big-thing-in-smartphones-the-software-1484139602, last checked by the author on January 12, 2017

[4] http://www.startribune.com/fda-says-st-jude-heart-devices-vulnerable-to-hacking/410153595/, last checked by the author January 12, 2017.

have is the increased chance of compromising our data. As the use of this technology grows, there are more and more opportunities for phishing, wireless hacking, etc. Thus, as frictionless computing becomes more prevalent it greatly increases the opportunity for the hackers to get at our 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 of us use our personal devices to access work information. We like to have remote access to notes apps like Evernote and cloud storage sites like DropBox. We text our clients and receive work emails, and that's all sent to/from our personal device. It's that same device that will be used to engage further in frictionless computing— many of us are probably Alexa addicts already, for instance. To date, we feel comfortable mixing business and personal use because we 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. I am concerned that the increased use of frictionless computing is hastening that change.

Today it might be reasonable to put a password to restrict access to the phones. But if frictionless computing is going to increase the opportunities for bad guys to hack into our devices, then it might not suffice to simply have a password or thumbprint barrier to access our phone. The prudent move might be to get another device all together for work matters. Maybe that work device won't be used for frictionless computing at all. Maybe the security measures we take with that work-only device will be more stringent than our personal device. Then, we 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 question we need to ask 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 we have crossed that line. 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.

5. Open Source Software. First— What IS open source software?

I'm thinking that this is your inner monologue right now: "So what exactly is this open source thing? If Rule 1.1 says that I need to understand it, then explain it to me." You got it. But rather than give you my layperson's description of the technology, here is the explanation from howtogeek.com.

Geeks often describe programs as being "open source" or "free software." If you're wondering exactly what these terms mean and why they matter, read on. (No, "free software" doesn't just mean that you can download it for free.)

Whether a program is open-source or not doesn't just matter to developers, it ultimately matters for users, too. Open-source software licenses give users freedoms they would not otherwise have.

(a) The Definition of Open Source

If a program is open-source, its source code is freely available to its users. Its users – and anyone else – have the ability to take this source code, modify it, and distribute their own versions of the program. The users also have the ability to distribute as many copies of the original program as they want. Anyone can use the program for any purpose; there are no licensing fees or other restrictions on the software. The OSI has a more detailed definition of "open source" on its website.

For example, Ubuntu Linux is an open-source operating system. You can download Ubuntu, create as many copies as you want, and give them to your friends. You can install Ubuntu on an unlimited amount of your computers. You can create remixes of the Ubuntu installation disc and distribute them. If you were particularly motivated, you could download the source code for a program in Ubuntu and modify it, creating your own customized version of that program – or of Ubuntu itself. Open-source licenses all allow you to do this, while closed-source licenses place restrictions on you.

The opposite of open-source software is closed-source software, which has a license that restricts users and keeps the source code from them. Firefox, Chrome, OpenOffice, Linux, and Android are some popular examples of open-source software, while Microsoft Windows is probably the most popular piece of closed-source software out there.

(b) Open Source vs. Free Software

Open source applications are generally freely available – although there's nothing stopping the developer from charging for copies of the software if they allow redistribution of the application and its source code afterwards. However, that's not what "free software" refers to. The "free" in free software means "free as in freedom," not "free as in beer." The free software camp, led by Richard Stallman and the Free Software Foundation, focuses on the ethics and morals of using software that can be controlled and modified by the user. In other words, the free software camp focuses on user freedoms.

The open-source software movement was created to focus on more pragmatic reasons for choosing this type of software. Open-source advocates wanted to focus on the practical benefits of using open-source software that would appeal more to businesses, rather than ethics and morals. Ultimately, both open-source and free software advocates are developing the same type of software, but they disagree on the messaging.

(c) Types of Licenses

There are many different licenses used by open-source projects, depending on which the developers prefer for their program. The GPL, or GNU General Public License, is widely used by many open-source projects, such as Linux. In addition to all the above definitions of open-source, the terms of the GPL specify that, if anyone modifies an open-source program and distributes a derivative work, they must also distribute the source code for their derivative work. In other words, no one can take open-source code and create a closed-source program from it – they must release their changes back to the community. Microsoft referred to the GPL as being "viral" for this reason, as it forces programs that incorporate GPL code to release their own source code. Of course, a program's developers can opt not to use GPL code if this is a problem.

Some other licenses, such as the BSD license, place less restrictions on developers. If a program is licensed under the BSD license, anyone can incorporate the program's source code into another program. They don't have to release their changes back to the community. Some people see this is being even more "free" than the GPL license, as it gives developers the freedom to incorporate the code into their own closed-source programs, while some people see it as being less "free" because it takes rights away from the end users of the derived program.

(d) Benefits for Users

This isn't all dry, unimportant stuff that only matters to developers. The most obvious benefit of open-source software is that it can be had for free. The example of Ubuntu Linux above makes that clear – unlike Windows, you can install or distribute as many copies of Ubuntu as you want, with no restrictions. This can be particularly useful servers – if you're setting up a server, you can just install Linux on it. if you're setting up a virtualized cluster of servers, you can easily duplicate a single Ubuntu server. You don't have to worry about licensing and how many instances of Linux you're allowed to run.

An open-source program is also more flexible. For example, Windows 8's new interface disappointed many long-time desktop Windows users. Because Windows is closed-source, no Windows user can take the Windows 7 interface, modify it, and make it work properly on Windows 8. (Some Windows users are trying, but this is a painstaking process of reverse engineering and modifying binary files.)

When a Linux desktop like Ubuntu introduces a new desktop interface that some users aren't fans of, users have more options. For example, when GNOME 3 was released, many Linux desktop users were equally turned off. Some took the code to the old version, GNOME 2, and modified it to make it run on the latest Linux distributions – this is MATE. Some took the code to GNOME 3 and modified it to make it work in a way they preferred – this is Cinnamon. Some users just switched to existing alternative desktops. If Windows was open-source, Windows 8 users would have more choice and flexibility. Just take a look at CyanogenMod, a popular, community-driven distribution of Android that adds features and support for new devices.

Open-source software also allows developers to "stand on the shoulders of giants" and create their own software. Witness Android and Chrome OS, which are operating systems built on Linux and other open-source software. The core of Apple's OS X – and therefor iOS – was built on open-source code, too. Valve is furiously working on porting their Steam gaming platform to Linux, as this would allow them to create their own hardware and control their own destiny in a way that isn't possible on Microsoft's Windows.

This isn't an exhaustive description – entire books have been written on this subject – but you should now have a better idea of what open-source software actually is and why it's useful to you.

(e) The Fundamental Ethics Problem

I think it's unethical for lawyers to use open source software for client work.

I want you to read that again. I said that I THINK it's unethical for lawyers to use open source software. Truth is, I'm not so sure. That, however, is how I'm leaning after doing a bit of research. Permit me to explain how I arrived at that conclusion….and please let me know if you agree. I'd love to hear what the lawyer-universe thinks.

First, my disclaimer. I am not a luddite. I am not scared of technology, and I don't want to discourage lawyers from using it. The question I'm grappling with is not, "Should lawyers be taking use of cutting edge technology like open source software." The question is, "Given the actual opinions and standards that exist, are lawyers violating the ethics rules by using open source software." So don't attack me for trying to be anti-technology, because I'm not.

In order to understand the ethical concern, you'll need a brief understanding about a key ethical concern with email. I'm sorry to bore you with the history lesson, but trust me, it's necessary.

Go back to the 90s when email first became popular. For those of use who are old enough to recall, lawyers couldn't use email in their practice because it was unencrypted. Our duty to safeguard client confidences per Rules 1.1 and 1.6 prohibited us from using the tool. The ABA and state bars across the country deemed that unencrypted email was too insecure and that lawyers who used it weren't taking the necessary steps to fulfill their duty of protecting clients' confidential information. So what changed? Today email is generally still unencrypted, but lawyers use it every day. Here's the change— congress criminalized the interception of email.

Once Congress made the interception of email a crime, the powers that be then agreed that lawyers had a reasonable expectation of privacy in using the medium. The key phrase is "a reasonable expectation of privacy." The ABA issue a formal opinion in 1999 confirming that idea:

> "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."

States have since 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 furor over gmail and other free email services back in 2008.

In it's Opinion 820, the New York State Bar Association opined about those free email systems. The systems were a concern because of the business model that the systems use to keep the service free. Here's how they work: in return for providing the email service, "the provider's computers scan e-mails and send or display targeted advertising to the user of the service. The e-mail provider identifies the presumed interests of the service's user by scanning for keywords in e-mails opened by the user. The provider's computers then send advertising that reflects the keywords in the e-mail." The obvious problem is that if we're using the email system for client work, then we're 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. They applied that same reasoning to the question of free emails.

Even though the email messages in the current systems are 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."

What the opinion is basically saying is that there continues to be a reasonable expectation of privacy in these email systems. Maybe the better way to phrase it is a reasonable expectation of "confidentiality," but the idea is the same. What's important to note is that the technology developed, but the standard that was applied remained the same.

If we take that standard and apply it to open source software, then…Houston, we have a problem. Earlier I noted that the characteristic that makes open source software "open" is that any programmer could change the source code. That's the whole point of open source software. But that ability to change the source code is what worries me.

If any programmer could change the code to an open source program, then isn't it possible that some version of that software could contain a virus or other nefarious element? What if the programmer installed a hidden web bug or other software device that allows the programmer to view, obtain, and otherwise see your confidential client information? Such a devious act isn't out of the realm of possibility. In fact, it seems realistic, and such tactics are being seen in the real-life practice today. Take the recent opinion out of Alaska.

In 2016 the state of Alaska issued an opinion that dealt with the ethical propriety of lawyers using web bugs to obtain information from their adversaries/opposing parties. The

Alaska authorities reviewed a case where an attorney actually utilized a bug and the Bar opined that using such tools would be an ethical violation because it "impermissibly infringes on the lawyer's ability to preserve a client's confidences as required by Rule 1.6." I realize that the opinion isn't really on point— in the open source question we're not talking about a lawyer installing a bug. I brought it up, however, because it shows that the use of those software devices is very much a reality in today's practice.

What if a programmer installs a similar type of software device in a piece of open source software and that device allows the programmer to view, copy, and disseminate your confidential client information? Getting hacked or taken advantage of doesn't give rise to ethical liability, per se. But there are opinions that have said that you have a duty to avoid the obvious scams. See New York City Bar Association Formal Opinion 2015-3, April 22, 2015 ("In our view, the duty of competence includes a duty to exercise reasonable diligence in identifying and avoiding common Internet-based scams, particularly where those scams can harm other existing clients."). Being infested with a virus/web bug certainly seems like an obvious concern, given the realities of the world today. The question is, should we have expected that to happen?

Should a reasonable lawyer have known that there is a realistic probability that some dangerous device could be installed in open source software? Should a reasonable lawyer have considered the open source software platform to be off limits because our client's information is too vulnerable in that way? Given the open nature of the software and given the real potential of having web bugs inserted into code, do lawyers have a reasonable expectation of privacy in open source software?

My answer is no.

It seems easy for a programmer to secretly install some bug or other information reviewing device. There are no controls or procedures that stop them from doing so. It is an

open opportunity for any bad actor to wreak havoc and there is very little to no protection against it.

A critical counter argument needs to be addressed. It is true that a programmer could still install some bug-like device even in a closed software environment. A programmer in Microsoft or Apple could do it, and we might never be the wiser. But I don't think the question is whether it could happen — the question is whether it is likely. One would think that the corporate software developer would have quality control measures that would ferret that out. There would be supervisory procedures to avoid that type of thing from happening. Given those measures, I would think that it's reasonable for lawyers to assume that there would not be a web bug installed in the corporate-purchased software. Even if it did occur, it would have to be some employee/programmer gone rogue. That sort of extraordinary circumstance could be detrimental to the client, but it wouldn't necessarily mean that the lawyer was derelict in their ethical duties by trusting the software. It could probably still be said that the lawyer had a reasonable expectation of privacy in that corporate/closed source-created software.

One could argue that there are informal quality control measures in the open source environment. There are apparently very strong ethical underpinnings to the open source movement. Behaving unethically is looked down upon in the open source community and there is a decent amount of peer pressure on programmers to uphold those unwritten ethical standards. My concern is that there is no actual mechanism to enforce it. The only thing stopping open source programmers from installing is the communal sense of morality that discourages such behavior. The lack of any formal mechanism is problematic.

It's the ability of almost any programmer at any time to manipulate the code that makes me believe that lawyers do not have a reasonable expectation of privacy when using open source software. Now, I realize that that is a blanket statement. There are likely to be a variety of factors that could alter the equation. For instance, maybe the main open source software

system of some sort could have excellent quality control. That's fine, but what about the plug-ins you may download to use in connection with that tool? Maybe some open source systems will be inherently more secure than others because the cooperative that developed it does adopt some quality control. Okay, so then maybe we con't have to avoid all open source software, just the sketchy ones. I'm sure that there are issues and I confess to not having an expert understanding of the programming world, so there are surely plenty of other considerations that I haven't accounted for.

Here, however, is why you should take my opinion seriously…even if you think it comes from a place of relative ignorance.

I have a decent understanding of technology. I also have a decent understanding of the ethics rules. Truth is, I probably have as much knowledge in both areas as any ethics investigator who would be evaluating a grievance. And if I'm leaning toward believing that open source software is an ethics violation, then that ethics investigator might be too.

Now….if someone who is reading the materials disagrees with this analysis, then please contact me and tell me why I'm wrong. But be polite.

Let's assume that I'm overracting. After all, there are some reputable companies that create a variety of OSS. Sun Microsystems makes Open Office, a tremendously popular OSS alternative to Microsoft's Office. Sun is now owned by Oracle, and one would have to assume that there is quality control there, right? So, for the sake of argument, let's say that there is a bunch of OSS that is probably reasonably safe, but a lot of it that might not be. In that case, the prohibition I mentioned above wouldn't be a blanket thing, it would only apply to some sketchy-type of OSS products. So how do we determine which OSS products are too "sketchy" as I so eloquently put it? I think we need to consult one of my favorite ethics opinions: California's Opinion 2010-179.

In that opinion the State of California gave us sone factors that I call the “Technology Permissibility Factors.” I gave them that name because I think you could use these factors to evaluate the permissibility of all kinds of new technology. Let’s take little diversion to discuss those factors and how they impact our future ethical duties

(f) The “Technology Permissibility Factors.”

In 2010 The State Bar of California presented us with California Formal Opinion No. 2010-179 (hereinafter “CO 2010-179”). While the impetus for the opinion was a discussion about a lawyer’s use of an insecure wireless connection to do client work, the opinion actually went far beyond that (in a good way). That opinion was primarily concerned about whether a lawyer could do client work on an unsecured network found in a coffee shop. They understood that the realities of work in the coffee shop meant that “without appropriate safeguards (such as firewalls, secure username/password combinations, and encryption), data transmitted wirelessly can be intercepted and read with increasing ease.” In making that statement they clearly realized that the issue was bigger than just working in a coffee shop and that what they were really addressing was the appropriate use of technology, in general. The drafters knew that they were in a tough spot and they acknowledged that, “unfortunately, guidance to attorneys on this area has not kept pace with technology.” The opinion, therefore, attempts to provide broader direction for lawyer. Opinion 179 actually sets forth some general guidance that helps lawyers navigate both existing technologies, as well as those that may arise in the future.

That California opinion has been cited by many other jurisdictions over the years, but one other state in particular has done an interesting application. In Wisconsin Formal Ethics Opinion EF-15-01 (hereinafter referred to as “WO 15-01”), that state bar reviewed the permissibility of using cloud computing in the practice of law. They stated that, “cloud computing is permissible as long as the lawyer uses reasonable efforts to adequately address

the potential risks associated with it." WO 15-01 at 2. The obvious question is, "what is reasonable?" According to Wisconsin, "To be reasonable, the lawyer's efforts must be commensurate with the risks presented by the technology involved, the type of practice, and the individual needs of a particular client." WO 15-01 at 9. But that's not all. The bar also reviewed the factors that California set forth in Opinion 2010-179, combined them with factors set forth in the commentary to Rules 1.6 (Confidentiality) and 5.3 (Supervision of Nonlawyer Personnel) and expanded upon them. Between those sources, lawyers have a handy bit of guidance for how to deal with other technologies that might arise in the future.

I call this collective list the "Technology Permissibility Factors." The factors could be helpful for all attorneys when evaluating the permissibility of new systems in the future. Below we'll discuss the factors, each followed by a bit of insight. However, I strongly encourage you to read the actual opinions as well as Rules 1.6 and 5.3 (and the commentaries I've noted herein) because they explain the factors more fully and it makes more sense after you read the text. In addition, there is a new opinion from the ABA (Opinion 477). That expands on these ideas and it should be reviewed as well. Here is my analysis of the Technology Permissibility Factors…

1— An attorney's ability to assess the level of security afforded by the technology, including…how the technology differs from other media use

Here's where understanding existing technologies becomes key. The only way to properly evaluate the risks of systems that have not yet been reviewed by disciplinary authorities is to compare them to the systems that have already been evaluated. To accomplish that, you need to understand the underlying technology. The mandate to have that knowledge comes right from the ethics code (Rule 1.1, Comment [8]):

> "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." *[emphasis added]*

Things you should be asking are: Are the risks the same? How are they different? Do the issues that were raised when disciplinary authorities opined on the existing technologies apply to these new systems?

2— An attorney's ability to assess the level of security afforded by the technology, including…whether reasonable restrictions may be taken when using the technology to increase the level of security…and the likelihood of disclosure if additional safeguards are not employed.[5]

If it's relatively easy to make things safer, then lawyers might wanted to consider taking additional safeguards. Of course, there are two parts to this factor— if those additional safeguards are not likely to make a difference, then there's no reason to put them into effect. But here is something to watch out for, and it illustrates why you need to stay on top of the industry standards.

What happens if a tool is developed which ends up being an easy way to enhance security but employing that tool is not likely to make much of a difference. However, what happens if most firms utilize that security technology and it ends up becoming an industry standard regardless of the relative effectiveness of the technology. Does the fact that it has been adopted industry-wide mean that a reasonable lawyer would be expected to utilize that system? It might be in our best interest to employ measures that have been adopted by the larger legal community even if we're not so sure that they will have an additional benefit, just so that we can say we are taking reasonable measures.

3— The cost of employing additional safeguards.[6]

Everything comes down to reasonableness. If the additional measures are super expensive, then we're not going to be expected to employ them. However, here is where I think we can have a discriminatory situation. What if there are some measures that are helpful and

---

[5] WO 15-01 at 10, citing Rule 1.6, Comment [18].

[6] WO 15-01 at 10, citing Rule 1.6, Comment [18].

expensive….but you have a firm that is large enough to afford those measures. Will there be a double standard? Maybe we will expect firms that could afford the measures to employ them, but firms that can not afford them will be off the hook. That wouldn't necessarily be "fair", but I can envision that disparate treatment occurring in real life.

4— The difficulty of implementing additional safeguards.[7]

5— The extent to which the additional safeguards adversely affect the lawyer's ability to represent clients.[8]

Are there tools available to increase security like complicated password generators, remote wipe capabilities for cell phones, and super-duper encryption techniques for websites? Sure. But at some point the utilization of those technologies create such an obstacle for a lawyer that it makes it tougher for them to get their job done. The more administrative layers that are created, the more steps that lawyers need to go through to employ the protections, the greater the likelihood that it will begin to affect their legal work. That's not to say that all of those safeguards should be thrown out, but it's another factor to consider in the overall analysis.

6— An attorney's ability to assess the level of security afforded by the technology, including…Limitations on who is permitted to monitor the use of the technology to what extent and on what grounds.

This combines two questions: First, what third parties will have access to the technology? This implicates Rule 5.3 and the duty to supervise those nonlawyer personnel. Also, do you need any assistance from technologically knowledgeable individuals to help you operate/secure the systems? If so, they may be monitoring the technology and they should be watched as well. In that regard you should keep in mind that our duty to supervise nonlawyer personnel is increasing. These days we are expected to supervise people who might have once been considered "independent contractors" and outside of our sphere of responsibility. I think

---

[7] WO 15-01 at 10, citing Rule 1.6, Comment [18]

[8] WO 15-01 at 10, citing Rule 1.6, Comment [18]

that's one reason why many rules have changed the title to Rule 5.3 from "Responsibilities regarding non-lawyer assistants" to "Responsibilities regarding non-lawyer *assistance*."

7— Legal ramifications to third parties of intercepting the information

This is a biggie. Remember that one of the main reasons that lawyers were ultimately permitted to use unencrypted email was because the interception of the information sought was criminalized. Only then was the lawyer considered to have a reasonable expectation of privacy in using the systems. If new systems arise and there are no legal ramifications to intercepting the information that travels through that system, then it's not likely to be ethically permissible. And this dovetails into the next factor…

8— The degree of sensitivity of the information

The California opinion says it best. "The greater the sensitivity of the information, the less risk an attorney should take with technology." Common sense. This is repeated in Rule 1.6, Comment [18]. A good practical example comes from the world of international espionage.

A few years ago, the BBC reported on information revealed by Edward Snowden. According to Snowden, foreign intelligence services were active monitoring a US law firm. Specifically, the article stated,

> "The February 2013 document says the Australian Signals Directorate monitored a US law firm used by the government of Indonesia for trade talks, according to the New York Times (NYT)…The Australians said that "information covered by attorney-client privilege may be included" in the intelligence they offered to share with the NSA, it says.[9]

Did you catch that? The Australian intelligence services were listening to the advice being given by a lawyer to it's client. They then offered that information to the NSA. None of the articles I read explained how, exactly, the conversations were monitored. Was is review of emails? Tapping of phones? What's clear, however, is that as new communication technologies are created, lawyers who deal with sensitive information might want to reconsider whether they

---

[9] http://www.bbc.com/news/world-us-canada-26216883, last checked by the author on June 21, 2016.

employ those technologies. If the substance of their discussions with their clients are likely to attract the attention of intelligence gathering agencies, then maybe lawyers should stick to face-to-face exchanges? It's certainly something to consider.

9— Possible impact on the client of an inadvertent disclosure or unauthorized interception of privileged or confidential information or work product, including possible waiver of privileges. CO 2010-179. Or as stated in WO 15-01 at 10, "the possible effect that inadvertent disclosure or unauthorized interception could pose to a client or third party."

Here's an example of how we need to think outside of the proverbial box. Consider the issue of texting our clients and whether it would be a good idea from a privilege point of view. We need to make sure that we keep the advice we give our client confidential in order to claim and preserve the attorney-client privilege. If the statements are revealed to a third party we lose that protection. It seems like it would be safe to text information to a client, given that the information is going directly to the client's phone. It's not like we're posting our messages on Facebook where all the world could see them. However, there could be a waiver issue nonetheless.

For instance, what if we know that the boyfriend of our unmarried client commonly reviews our client's text messages. If we are aware that the information we text to our clients is likely to be viewed by a third party, then aren't we jeopardizing privilege? You could argue that it's no different from emails. Any message sent to the client's phone could be viewed by another party, thereby blowing privilege. Of course, I don't see how that helps you—it just gives further credibility to the argument that maybe we shouldn't be using these technologies to send messages.

I'm not sure how this will play out, but these are the things we need to watch out for when it comes to evaluating new technologies.

10— The need for increased accessibility and the urgency of the situation.[10]

---

[10] This is a combination of the factors in both the California and Wisconsin opinions.

The California opinion gives concise and valuable guidance on this factor. "If the use of technology is necessary to address an imminent situation or exigent circumstances and other alternatives are not reasonably available, it may be reasonable in limited cases for the attorney to do so without taking additional precautions."

11— The experience and the reputation of the service provider.[11]

12— The terms of agreement with the service provider.[12]

You have GOT to check the terms of service. Most lawyers don't appreciate that the terms of service are a contract. It's an actual agreement that sets forth the legal rights of the parties who provide and use the technology. Read it— don't just check the box that says, "I agree" and move on. Read the actual terms.

13— The legal and ethical environments of the jurisdictions in which the services will be performed particularly with regard to confidentiality.[13]

If you're using a technology and storing client information on that provider's servers you need to ask questions like, "Where are those servers located?" They might be in foreign jurisdictions which give the provider the right to review, own, or disseminate that information.

14— Client instructions and circumstances

The California opinion states that if a client tells us not to use a certain technology, we can't use it. Got it.

Wisconsin clearly agrees because their opinion states, "A lawyer must follow the client's instructions unless doing so would cause the lawyer to violate the Rules of Professional Conduct or other law. Moreover, a lawyers should consider any circumstances that may be relevant. Fort example, if the attorney is aware that other people have access to the client's

---

[11] WO 15-01 at 10, citing Rule 5.3 Comment [3].

[12] WO 15-01 at 10, citing Rule 5.3 Comment [3].

[13] WO 15-01 at 10, citing Rule 5.3 Comment [3].

decides or accounts and may internet the client information, the attorney should consider that in assessing the risk." WO 15-01 FN 27, citing CO 2010-179.

Back to the open source software issue…

I think a lawyer could use these factors when evaluating whether a particular piece of OSS is reputable enough to use. Critical questions wold then be asked like: What is the security afforded by the developer? Will you be using it to process client confidential information or otherwise sensitive info? Is your client ok with using the platform? All of that would help ascertain whether a particular piece of OSS might be okay for a lawyer to use.

So….if there are some pieces of OSS that are okay to use, what are some other ethical concerns that might face lawyers when they employ that software in their practice?

(f) The Duty to See Problems Coming

What if you use a piece of OSS that seems reputable, but a rogue developer installed some bug that (for instance) stole client confidential information…will you get in trouble? There haven't been any opinions on point, but there is some guidance that we find— and it comes down to a question of competence. Incidentally, the concept I'm about to explain — what I call the duty to avoid scams — is not limited to open source software. We'll touch on that a bit more in the program.

There are a variety of opinions that have held that lawyers have a duty to understand the dangers of the internet. The Association of the Bar of the City of New York Committee on Professional Ethics gave us Formal Opinion 2015-3 in April 2015 which dealt with email scams. When discussing that particular type of theivery, the opinion listed a series of troubling indicators that might have raised concern for the lawyers and said that the lawyer should have seen them coming. In reviewing those factors, the committee said, "A lawyer's suspicion should be

aroused by any one or more of these common "red flags" indicating a scam…" That committee didn't come out and say it explicitly, but it made it clear that a lawyer has a duty to take reasonable steps to avoid an obvious internet scam.

Another case in Rhode Island dealt with a similar issue. There a lawyer acted as a "Pay Master," or an escrow agent for a client he found online. The client gave the lawyer money to deposit in his trust account, then had him disburse those funds to others. The lawyer asked Rhode Island disciplinary counsel for an opinion about whether the scheme was permitted, and counsel basically said, yeah, it could be, but be careful because it's likely to be a scam. Of course, it was a scam and the lawyer was disciplined. In the Matter of Donald F. DeCiccio., No. 2013-275-M.P. The Rhode Island Supreme Court Supreme Court didn't give us a slam-dunk holding to quote, but they found that the lawyer violated the rule on competence. Basically, they said he should have known better.

These cases say to me that there lawyers have a duty to see obvious scams coming. What happens if there's a bad programmer who installs a virus on an open-source program (say, for example, an open source widget that someone might download to use with their Wordpress blog). Isn't it sort of obvious that such a scenario could occur? The question becomes whether it's reasonable to foresee those bad actors. Are rogue OSS developers the equivalent of an email internet scammer? My opinion (which isn't worth a whole lot, I'm sure) is that they are not the same. At least, not yet. I don't think the dangers are so obvious in the world of OSS. But it could change overnight. The more these forms of software become integrated with the practice of law and the more people get into trouble, then the more likely lawyers will be expected to be aware of the dangers associated with OSS.

(g) Violating Copyrights

Many people mistakenly believe that OSS is the wild-west of technology and that no rules apply. That's certainly not the case. As we will discuss in the program, there are a variety

of licenses that attach to open source software. With those licenses come copyright issues. From an ethical perspective, we need to consider whether violating those copyrights constitutes a breach of the code. It seems to come down to a question of whether you know — or should have known — that you were violating the law.

If you know that you are using OSS in violation of it's licensing agreement or copyrights, then you might be committing copyright infringement. That happens to be a crime and a violation of that law would probably invoke Misconduct issues. In particular, Rule 8.4(b).

> Rule 8.4. Misconduct (in part)
>
> It is professional misconduct for a lawyer to:
>
> (a) violate or attempt to violate the Rules of Professional Conduct, knowingly assist or induce another to do so or do so through the acts of another;
> (b) commit a criminal act that reflects adversely on the lawyer's honesty, trustworthiness or fitness as a lawyer in other respects;
> (c) engage in conduct involving dishonesty, fraud, deceit or misrepresentation;
> (d) engage in conduct that is prejudicial to the administration of justice;

Of course, when reviewing 8.4(b) one can see that the criminal act needs to reflect adversely on the offender's fitness as a lawyer. To get some guidance there, we go to the commentary:

> Rule 8.4, Comment [2] Many kinds of illegal conduct reflect adversely on fitness to practice law, such as offenses involving fraud and the offense of willful failure to file an income tax return. However, some kinds of offenses carry no such implication. Traditionally, the distinction was drawn in terms of offenses involving "moral turpitude." That concept can be construed to include offenses concerning some matters of personal morality, such as adultery and comparable offenses, which have no specific connection to fitness for the practice of law. Although a lawyer is personally answerable to the entire criminal law, a lawyer should be professionally answerable only for offenses that indicate lack of those characteristics relevant to law practice. Offenses involving violence, dishonesty, breach of trust, or serious interference with the administration of justice are in that category. A pattern of repeated offenses, even ones of minor significance when considered separately, can indicate indifference to legal obligation.

If a lawyer willfully violated copyright law, I think that would qualify as the type of "dishonest" behavior envisioned by the rule/commentary. Nearly every lawyer understands that

copyright law exists, even if we don't have an expertise in the subject. A purposeful violation of that law is likely to be one of the "offenses that indicate lack of those characteristics relevant to law practice." Rule 8.4, Comment [2].

What if you didn't know that you were violating the copyright protections afforded to the OSS you're using because you didn't know about the type of license/copyright involved or you didn't understand what it meant? The question becomes whether you should have known that there was a potential violation. Then I think it's all about competence and the jury, as they say, is still out. Is reasonable to assume that the average lawyer would understand the OSS license distinctions? Is it reasonable to expect a lawyer to understand the OSS license distinctions? I don't know how an ethics committee will come down on that- no one does. Do yourself a favor and just become familiar with it and you won't have to worry about that problem.

6. Artificial Intelligence

The expanding duty of competence requires that we understand AI. Artificial intelligence is best described by going to a common reference book. Merriam-Webster diction defines it as: "an area of computer science that deals with giving machines the ability to seem like they have human intelligence" and "the power of a machine to copy intelligent human behavior."

Basically, AI is used to conduct what many refer to as routine tasks which normally takes several people many hours to perform. The unique part about this technology is that it tries to mimic human intelligence as it performs the tasks. It factors in all sorts of variables and it's "able to perform tasks that normally require human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages" (definition from Google). In the practice of law we're seeing AI used substantially in complicated e-discovery matters. The systems are able to conduct intricate document review processes which would

normally take associates or support staff oodles of hours to perform. That's one reason why the tasks, while intensive, are also sometimes referred to as "routine."

a. Confidentiality

There are already indications that AI can be used in improve speech recognition programs. In that regard, can't you see it being helpful in better dictation systems? On the speech recognition issue, the ethics issues to be concerned with include:

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

I think it's pretty clear that those questions all raise issues of confidentiality, Rule 1.6. If the speech is being recorded and disseminated, then you could be violating the duty to keep client information confidential. In addition, consider the privilege implications. If some vendor is getting access to information that is covered by privilege, then then dissemination of it could amount to a waiver of the privilege (which, most likely, you had no authority to waive). Let's take a moment to explore how Rule 1.6 is built a bit because it's important to understand that if you're going to apply it to AI (or any technology issue)

When I teach the rule on confidentiality, I tell my classes that the rule is broken down as follows: There's the general rule, then there are the "two permissions and the exceptions." The idea that we need to keep our information confidential is as elementary as they come. The tougher part is navigating when you are permitted (or required) to reveal information.

The rule states that we can reveal information if we have either express or implied permission. In 1.6(a) we are told that we can reveal information if the client gives "informed consent," which is what I call express permission." We can also reveal if "the disclosure is

impliedly authorized to carry out the representation." Obviously, that's the implied permission. Here's the whole rule:

> Rule 1.6. Confidentiality of information
> (a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation, or the disclosure is permitted by paragraph (b).
> (b) A lawyer may reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary:
> (1) to prevent reasonably certain death or substantial bodily harm;
> (2) to prevent the client from committing a crime or fraud that is reasonably certain to result in substantial injury to the financial interests or property of another and in furtherance of which the client has used or is using the lawyer's services;
> (3) to prevent, mitigate, or rectify substantial injury to the financial interests or property of another that is reasonably certain to result or has resulted from the client's commission of a crime or fraud in furtherance of which the client has used the lawyer's services;
> (4) to secure legal advice about the lawyer's compliance with these Rules;
> (5) to establish a claim or defense on behalf of the lawyer in a controversy between the lawyer and the client, to establish a defense to a criminal charge or civil claim against the lawyer based upon conduct in which the client was involved, or to respond to allegations in any proceeding concerning the lawyer's representation of the client; or
> (6) to comply with other law or a court order.

One of the trickier things to navigate in the world of confidentiality is to know when something is "impliedly authorized" as set forth in subsection (a). One can envision that the issue would arise in a negotiation context, perhaps. Maybe your client would give you direction in the form of parameters, or they might talk to thou about their objectives and goals. Then, they'll set you free! Well, sort of…they'll let you enter into negotiations and ask that you proceed in furtherance of their goals. During the course of your conversations with your adversary, you might need to reveal some confidential information, if it's critical to achieving the client's objectives and also consistent with the client's directives. You might not have explicit direction to reveal particular confidential information, but it might be impliedly authorized to complete the negotiation.

The negotiation setting is a hypothetical example. But as we can see from the code, there are other instances that also impact the "impliedly authorized" concept and they're specifically mentioned in certain rules. Take Rule 1.14 as an example:

> Rule 1.14. Client with diminished capacity
> (a) When a client's capacity to make adequately considered decisions in connection with a representation is diminished, whether because of minority, mental impairment or for some other reason, the lawyer shall, as far as reasonably possible, maintain a normal client-lawyer relationship with the client.
> (b) When the lawyer reasonably believes that the client has diminished capacity, is at risk of substantial physical, financial or other harm unless action is taken and cannot adequately act in the client's own interest, the lawyer may take reasonably necessary protective action, including consulting with individuals or entities that have the ability to take action to protect the client and, in appropriate cases, seeking the appointment of a guardian ad litem, conservator or guardian.
> (c) Information relating to the representation of a client with diminished capacity is protected by Rule 1.6. When taking protective action pursuant to paragraph (b), the lawyer is impliedly authorized under Rule 1.6(a) to reveal information about the client, but only to the extent reasonably necessary to protect the client's interests.

This rule governs our actions when dealing with a client that might be of diminished capacity. The rule tells us that we have the ability to take protective action on behalf of such clients, if warranted. The rule also acknowledges that we may be forced to reveal otherwise confidential information when seeking that protection. For instance, we might have to tell a therapist if a client was threatening to harm themselves, or if they will suffer financial harm, we may need to tell a potential conservator about the location of assets. Are we permitted to do so? Subsection (c) is the part of the rule that's invoked. Those situations would likely be disclosures that are impliedly authorized, and (c) gives us specific permission in that regard.

The key reason for bringing up that section, however, is to explain how revelation might be impliedly authorized. The other ways you might be permitted to reveal confidential information fall into the exceptions of 1.6(b). But remember, it's not always about revealing confidential information — the other issue about confidentiality revolves around our "using" that

information. One can review the rules on conflicts to see what I mean. Rule 1.8 prohibits us from using information that we learn from a client to their detriment. 1.8(b) states:

> "A lawyer shall not use information relating to representation of a client to the disadvantage of the client unless the client gives informed consent, except as permitted or required by these Rules."

One can understand how "use" differs from "reveal." For instance, we might learn that a client is negotiating to buy a piece of property at a very discounted price. We may be tempted to try to purchase that property for ourselves, once we know that such a good deal is available. That would hurt our client if we either deprived them of the business opportunity, or if our bid caused the price the client needed to pay to be increased.

I always worry about confidential information when I think about new technology and I think it's worth inserting a waning in that regard. So much of this new technology shares information. This, of course, dovetails with the section above on "big data." It seems easy for one system to share our client's confidential information with another without us being aware. That's where the revelation of confidential information is a problem. But I think the "use" is also an issue. This is going to stray from the AI topic at hand, but it's still about technology and I think it's important.

Lawyers often have have confidential information on the whereabouts of a client's financial assets. That information often causes a lawyer to be conflicted out of a case because if they use that information on behalf of another client they would be using confidential information to the detriment of the client in violation of Rule 1.8. I think that, in the future, there will be a similar issue with a lawyer's knowledge of the location of a client's technological assets. I think that in the future clients will be moving information to various places, whether it be in the cloud, or offsite storage, or places that have not yet been created. After all, we can see that data is king…and it's valuable. For that reason I think there will be reason for them to clients to want to keep the location of that data a secret. Or maybe it's more than the location of the data- maybe

it's the systems that they use to collect that data. In either case, that could cause a conflict for lawyers in the future. Just as we can be conflicted out of a matter because we have confidential information about the location of a client's financial assets (which we might use that to their disadvantage) so too could we be conflicted out of a matter because we have confidential information about the location of a client's technological assets.

b. Supervision

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."[14]

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 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

---

[14] 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.

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.

All of that being said, AI isn't going to eliminate lawyers all together. Artificial intelligence can never actually substitute for the advice that a lawyer provides to a client. It could assist in trying to predict outcomes, but the conversation — the consultation — that must occur before a client makes a big decision can not be offloaded to a computer. There are far too many emotional, political, and perhaps public relations considerations that must be taken into account. (See Rule 2.1, which mandates that those other factors be considered in our legal advice to clients). I believe that the wise lawyer will recognize the areas where the practitioner can provide value to a client and focus their efforts (and their marketing plans) in those areas.

As far as the ethics issues…I'm not overly concerned about the other ethical issues that lawyers will face when *using* AI. The competence, communication, and confidentiality issues aren't so tough to grasp. I am concerned about the ethics issues that existing lawyers will face when responding to the changes like artificial intelligence. Not so much the new lawyers—there's nothing for them to "adapt" to, since they're just coming into the practice. I'm worried that a downward pressure on fees and a need to learn about new technology matters will cause veteran lawyers to misbehave more.

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

c. Who calls the shots?

Here's the last thing I want to mention about AI, and it also applies to much of new technology. That is…who gets to decide when we use it? Is the use of technology an objective of the representation, or a means…and why does that matter. For that, we need to review Rule 1.2, which discusses the allocation of decision making authority between lawyer and client.

Generally, Rule 1.2 tells us that the clients makes decisions about the objectives of the representation and the lawyer gets to decide the means. But the difference between the two are not laid out in the rules (or the comments). On the plus side, there is a bit of direction

regarding the criminal context. In those cases the rule tells us that we must abide by the client's decision when entering pleas, waiving jury trial and deciding whether to testify. But there is no direction when it comes to technology.

> Rule 1.2. Scope of representation
> (a) Subject to paragraphs (c) and (d), a lawyer shall abide by a client's decisions concerning the objectives of representation and, as required by Rule 1.4, shall consult with the client as to the means by which they are to be pursued. A lawyer may take such action on behalf of the client as is impliedly authorized to carry out the representation. A lawyer shall abide by a client's decision whether to settle a matter. In a criminal case, the lawyer shall abide by the client's decision, after consultation with the lawyer, as to a plea to be entered, whether to waive jury trial and whether the client will testify.
> (b) A lawyer's representation of a client, including representation by appointment, does not constitute an endorsement of the client's political, economic, social or moral views or activities.
> (c) A lawyer may limit the scope of the representation if the limitation is reasonable under the circumstances and the client gives informed consent.
> (d) A lawyer shall not counsel a client to engage, or assist a client, in conduct that the lawyer knows is criminal or fraudulent, but a lawyer may discuss the legal consequences of any proposed course of conduct with a client and may counsel or assist a client to make a good faith effort to determine the validity, scope, meaning or application of the law.

So, is technology an objective or a means? I can foresee situations where it might be both. There's an easy way to get around this, of course. Simply talk to your client. If you have the appropriate consultation with them per Rule 1.4 (as referenced in 12(a) above), then you're going to be fine.