COMMENT: ALEXA, TRANSMIT CLIENT DATA TO AMAZON: ETHICAL CONSIDERATIONS FOR ATTORNEYS LOOKING FORWARD TO VIRTUAL ASSISTANTS

Whitney L. Hosey†

I. INTRODUCTION ................................................................. 52
II. IS BIG BUSINESS WATCHING? HOW A.I. SYSTEMS COLLECT AND STORE DATA.................................................. 52
III. ALEXA, CAN CONVENIENCE BE ETHICAL? ............ 57
IV. ETHICAL TECHNOLOGY AND THE EVOLVING WORKPLACE ............................................................................ 66
   A. RECOMMENDATION 1: WHEN OPERATING IN SECURE WORKSPACE DEVICES SHOULD BE UNPLUGGED BEFORE ENGAGING IN ANY ORAL COMMUNICATION............................................. 68
   B. RECOMMENDATION 2: PLATFORMS LIKE AMAZON AND GOOGLE COULD DEVELOP SECURE CLOUD SPACE. .......................................................... 68
   C. RECOMMENDATION 3: BE AWARE AND BE OPEN WITH THE CLIENT. ................................................................. 69
V. CONCLUSION ............................................................................ 71

† © 2019 Whitney Hosey is a J.D. Candidate, Wake Forest School of Law where she currently serves as the Editor-in-Chief of the Journal of Business and Intellectual Property Law. Whitney is a graduate of the University of Virginia where she earned her B.A. in History and Government. Whitney would like to thank Professors Simone Rose and Abigail Perdue for their editing and writing assistance. She would also like to extend her sincere gratitude to the Journal’s incredible Board of Editors and Staff. Finally Whitney would like to thank her family and friends for their unending support and love.
I. INTRODUCTION

Amazon’s Alexa is moving beyond the home into offices, cars, and PC’s, and even in your vacuum cleaner. 1 Amazon continues to advertise Alexa as a virtual assistant capable of helping with everyday tasks. 2 But Amazon’s next target is business. 3 Amazon is not the only company looking to push artificial intelligence (A.I.) in the workplace. Both Cisco and Microsoft have also developed their own virtual assistants. 4 The current “Amazon for Business” platform is aimed at basic tasks such as booking meetings, but as the technology develops, so may its functional capabilities via its voice recognition and processing software. 5 Business software companies and computer companies are already integrating these systems into their programs to make the transition smoother. 6

This comment focuses on the need for attorneys, whose positions require a high level of confidentiality, to consider their ethical obligations as these technologies become more prevalent in society. 7 Part II provides an overview on how technologies like Amazon’s Alexa function. 8 Part III analyzes the applicable American Bar Association’s Model Rules of Professional Conduct (Model Rules) and how some state bar associations have handled changes in technology. 9 Finally, to avoid ethical violations, Part IV offers a few suggestions for attorneys who might consider purchasing or already have an A.I. device for their office.

II. IS BIG BUSINESS WATCHING? HOW A.I. SYSTEMS COLLECT AND STORE DATA

A.I. is defined as “a branch of computer science dealing with the simulation of intelligent behavior in computers.” 10 Usually intelligence

---

2 See id.
3 Id.
5 Finnegan, supra note 1.
6 Id.
7 See infra Part V.
8 See infra Part II.
9 See infra Part III.
10 Artificial Intelligence, MERRIAM-WEBSTER’S COLLEGIATE DICTIONARY (11th continued . . .
refers to the concept of human intelligence.\textsuperscript{11} The end goal of A.I. is to advance the technology so that it can “reason, learn, self-collect information, create knowledge, communicate autonomously, and manipulate their environment in unexpected fashions.”\textsuperscript{12} In other words, A.I. developers are looking to eventually replace or enhance certain human professional functions with machines.\textsuperscript{13} A.I. systems are complex and within the field there are various classifications and distinctions between platforms.\textsuperscript{14} One category of A.I. known as “strong” allows these machines to “think, reason, and deduce” in a manner at least similar to the human brain.\textsuperscript{15} As of right now, there is no “strong” A.I. available for commercial use, but an example would be a developer programming a computer “to have perception, beliefs and have other cognitive states that are normally only ascribed to humans.”\textsuperscript{16} The most prominent classification of A.I. in the current market is “weak” A.I., which is when the computer or system mimics human activity without the ability to actually reason or think for itself.\textsuperscript{17} An example of “weak” A.I. is Apple’s auto-correct feature, which is able to assess the user’s intended spelling and automatically correct the error.\textsuperscript{18} Because “strong” A.I. systems are not prevalent in the market, this comment will only focus on “weak” A.I. systems.

Commercially available systems like Amazon’s Echo Dot Alexa, Google Home, and Apple’s Siri are “weak” A.I. devices which leverage “automatic speech recognition (ASR) and natural language understanding (NLU) engines that enable a system to instantly recognize and respond to voice requests.”\textsuperscript{19} These systems can help users with daily tasks such as setting reminders, adding calendar meetings, and even providing up to date traffic information for the user’s common route.\textsuperscript{20} When triggered by the wake word, these

\textsuperscript{12} Id. at 5.
\textsuperscript{13} Id.
\textsuperscript{14} See generally id. at 5–8 (discussing the two categories of A.I. and each categories’ A.I. applications).
\textsuperscript{15} Id. at 6.
\textsuperscript{17} Ben-Ari et al., supra note 11, at 7.
\textsuperscript{18} See id. at 8 (suggesting that “weak” A.I. includes word processing programs that automatically correct spelling).
\textsuperscript{20} Hillary Brill & Scott Jones, Little Things and Big Challenges: Information continued . . .
devices actively engage with the user and “either stream or record the voice requests to servers which access the requests and form responses.”

The wake word varies from system to system, but generally there are multiple ways to activate the device.

The problem is that unless you manually turn these devices’ microphones off they are always listening, even if it is passively. Alexa actually starts recording “a fraction of a second” before the wake word, and Google Home “listens to snippets of conversations” in order to be instantly responsive at all times. The information is then stored for approximately sixty seconds so the responses can be “situationally aware and ‘instant.’” In-home devices are not the only pieces of technology listening. In fact, Apple’s Siri comes to life by simply holding the home button, connecting the device to a user’s car, or saying “Hey Siri.” It is also important to note that these devices are not just listening for the specific device owner’s voice. Instead, Siri may be activated by anyone in the vicinity saying its name. And it’s not just Apple, some Samsung Galaxy users have commented that Samsung’s A.I. assistant Bixby is automatically activated at random, meaning it too is passively listening. Even more disturbing is Alexa’s recent bout with the giggles, where Alexa users have heard unprompted laughter coming out of their Alexa device. These devices are becoming more

---

21 Peggy Wojkowski, Alexa, Am I Violating Legal Ethics?, CHI-KENT C. L. INST. FOR SCI. L. & TECH. BLOG (May 31, 2017), blogs.kentlaw.iit.edu/islat/2017/05/31/alexa-violating-legal-ethics/. A “wake word” or wake-up term is the phrase or utterance which transitions the system from passive to active listening. See also Jules Polonetsky & Stacey Gray, The Internet of Things as a Tool for Inclusion and Equality, 69 FED. COMM. L.J. 103, 115 (2017).


23 Id.

24 Id.

25 Palmer, supra note 19.

26 Boughman, supra note 22.


28 See Boughman, supra note 22.

29 See id. See also, e.g., u/MSFT1776, Discussion, Anybody’s Bixby Getting Activated Randomly?, REDDIT (Sept. 20, 2018, 3:07 PM), https://www.reddit.com/r/GalaxyS8/comments/6odl1t/discussion_anybodys_bixby_getting_activated/.


continued . . .
prevalent. As of December 2017, Amazon reported that it has sold “tens of millions of Alexa-enabled devices.” According to Amazon, allegedly it is erased and replaced with the next sixty seconds of audio recording. However, per Alexa’s terms of use agreement, “if you access third-party services and apps through Alexa, Amazon can share the content of your requests with those third parties.” Interactions with Alexa such as voice recordings and searches are stored on the cloud, an accessible area where information is stored on the Internet instead of a user’s computer. Thus, the information in the cloud is potentially subject to subpoena like any phone record or browser history.

The distinction between what is and what is not stored is that until the wake word is spoken neither Amazon or Google are storing the everyday conversations of individuals in the room. Instead the data that is stored is anything spoken, searched, or overheard when the device is actively listening. “Amazon handles the information received from Alexa in accordance with its privacy policy.”


33 Palmer, supra note 19.

34 Boughman, supra note 22.


36 Amazon refuses to comply with an Arkansas Judge’s order to release audio data from a murder suspect’s artificially intelligent speaker to Arkansas authorities. No decision has been made as to whether Amazon will be forced to comply. David Lohr, Amazon Refuses to Comply with Police Request in Arkansas Murder Case, HUFFINGTON POST (Dec. 28, 2016, 7:14 PM), https://www.huffingtonpost.com/entry/amazon-arkansas-murder-case_us_58642d86e4b0eb586488082c; Palmer, supra note 19.


38 Boughman, supra note 22.

39 Id. continued...
companies discourage deleting interaction histories because it reduces the ability to create a profile with personalized features.\textsuperscript{40}

Many users purchase “weak” A.I. systems for in home use; however, commercial A.I. developers like Amazon are now pushing for businesses to take advantage of these systems in order to make their offices more efficient and productive.\textsuperscript{41} In fact, Amazon is so focused on getting Alexa into businesses that Amazon worked with Thomas Reuters Elite Workspace group to develop the Workspace Assistant.\textsuperscript{42} The system includes a billable hours feature which allows users to track their billable hours simply by saying “Alexa, track my time.” \textsuperscript{43} Workspace Assistant only works within the Workspace platform rather than relying on Amazon itself.\textsuperscript{44} According to a statement by Eric Ruud, Managing Director of Thomas Reuters Legal Enterprise Solutions, while the system may leverage Amazon’s technology, Workspace Assistant “always [operates] within the firm’s security walls.”\textsuperscript{45}

Always-on devices provide many convenience benefits to users. Not only can they be helpful in assisting with daily routine, but now they can also visibly show you the five-day forecast, make video calls, and play a user’s favorite music video.\textsuperscript{46} However, there are many risks associated with this technology as well, including the ability to create unique profiles on individuals, and store information which can potentially be leveraged against them in a legal proceeding.\textsuperscript{47}

There is a vast array of literature available regarding the privacy concerns of individuals.\textsuperscript{48} Nonetheless, what appears to be missing, and what this comment will address, is the ethical dilemma an attorney faces when deciding whether convenience in the form of a “weak” A.I. system, even one developed by Reuters, is prohibited by the Model Rules surrounding communication, storage of confidential client or prospective client information, and responsibilities regarding non-lawyer assistants.\textsuperscript{49} Part III below addresses which Model Rules may

\textsuperscript{40} Id.
\textsuperscript{41} See Finnegan, supra note 1.
\textsuperscript{43} Id.
\textsuperscript{44} Id.
\textsuperscript{45} Id.
\textsuperscript{46} David Pierce, Review: Amazon Echo Show, WIRED (June 16, 2017, 12:00 PM), https://www.wired.com/2017/06/review-amazon-echo-show/.
\textsuperscript{48} See, e.g., Bohn, supra note 47; Brill & Jones, supra note 20.
\textsuperscript{49} See infra Part IV.
be implicated in this decision.50

III. ALEXA, CAN CONVENIENCE BE ETHICAL?

The Model Rules of Professional Conduct were promulgated by the American Bar Association in 1983 in order to provide attorneys and legal professionals with a baseline standard for legal ethics and professional responsibility.51 While the ABA Model Rules themselves are recommendations which states may choose to adopt, as of 2015, forty-nine of the fifty United States have adopted them in whole or in part.52 California is the only state that has not adopted the Model Rules in any fashion.53 It is important to note that other statutes and court-created laws also govern attorney behavior outside of the Rules an attorney’s state adopts.54 While some jurisdictions may differ slightly, the Model Rules still serve as a resource to refer to when deciding whether having an A.I. system like Alexa or Google Home in a legal office is ethical (the ethical dilemma). Specifically, Model Rules 1.4, 1.6, 1.18, and 5.3 are significant.55 Model Rule 1.4(a)(1) states in relevant part that a “lawyer shall promptly inform the client of any decision or circumstance with respect to which the client’s informed consent (…), as defined by rule 1.0(e), is required by these Rules.”56 Model Rule 1.0(e) provides the definition of “informed consent” as “the agreement by a person to a proposed course of conduct after the lawyer has communicated adequate information and explanation about the material risks of and reasonably available alternatives to the proposed course of conduct.”57 The first step in satisfactorily following Model Rule 1.4(a)(1) is figuring out when informed consent is required.58 Informed consent is required when a rule states the client must give informed consent.59 An attorney must inform the client “about the

---

50 See infra Part III.
53 Id.
54 PEARCE ET AL., supra note 51, at 8.
55 See infra Part III.
56 MODEL RULES OF PROF’L CONDUCT r. 1.4(a)(1) (AM. BAR ASS’N 2016).
57 Id. at r. 1.0(e).
59 See, e.g., MODEL RULES OF PROF’L CONDUCT r. 1.6(a) (AM. BAR ASS’N 2016)
advantages and disadvantages of revelation in language the client can understand." Under some rules informed consent must be expressly given in writing, while others allow for implied authorization as long as the attorney has properly informed the client about his or her rights. Regardless, “informed consent requires an understanding of the risks and benefits” of the client’s pending decision. An ethical attorney fulfills his or her professional obligation only when he or she provides the proper information, informs the client of the risks associated with following the attorney’s proposed course of action, and then provides alternatives all within a reasonable time frame.

Model Rules 1.0(e) and 1.4(a)(1) act as important red flags to attorneys, signaling that when the words “informed consent” are used in another Model Rule, the attorney must remain vigilant in his communication. This leads directly to the next Model Rule implicated in the ethical dilemma, which is Model Rule 1.6(a). Model Rule 1.6(a) states that 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).” Model Rule 1.6(b) then goes on to explicitly state when disclosure is permitted, allowing disclosure for the purposes of preventing the client from coming to harm if the information is not disclosed, preventing harm to others, or protecting the lawyer himself or herself in a legal controversy.

Model Rule 1.6 is implicated in the ethical dilemma because unless

(continued . . .)
a client explicitly elects to disclose information relating to the lawyer’s representation of himself or herself to a third party, or one of the exceptions in Model Rule 1.6(b) is triggered, then the lawyer must not reveal information.\(^{68}\) Although, in some circumstances the disclosure is implied if revelation is required as part of representation.\(^{69}\) The comment to Model Rule 1.6 is helpful in establishing the purpose of limiting information shared with others.\(^{70}\) Comment Two notes that clients need “to communicate fully and frankly with the lawyer even as to embarrassing or legally damaging subject matter.”\(^{71}\) Therefore, it follows that if a client is encouraged to share embarrassing or other confidential subject matter, the attorney should be able to ensure that third parties will not be able to leverage that information against them.\(^{72}\) Comment four to Model Rule 1.6 further emphasizes that “this prohibition also applies to disclosures by a lawyer that do not in themselves reveal protected information but could reasonably lead to the discovery of such information by a third person.”\(^{73}\)

Assurances that information from privileged client meetings will not be disclosed would be difficult to achieve with always-on technologies like Alexa or Siri present.\(^{74}\) These devices can be triggered with relative ease, as noted in Part I \(^{75}\); therefore, unless the attorney were to disclose that he or she owned one of these devices and the client consented to their use, or if the attorney took steps to manually deactivate the device, the attorney would likely violate Model Rule 1.6(a).\(^{76}\) The violation arises when the always-on device hears or thinks it hears the wake word, causing the device to record and transmit the data back to the cloud, which is owned by Amazon—a third party.\(^{77}\) As emphasized in Part I, Amazon uses all data collected to create profiles and even transmits data to other third parties.\(^{78}\) This means that the attorney has inadvertently revealed information pertaining to a client, without the client’s consent and thus he or she is in violation of Model Rule 1.6.\(^{79}\)

The next Model Rule implicated in the ethical dilemma is Model Rule 1.18(a) and (b), which outline the duties owed to a prospective

\(^{68}\) See id. at r. 1.6(a).

\(^{69}\) Id.

\(^{70}\) See id. at r. 1.6 cmt. 1.

\(^{71}\) Id. at r. 1.6 cmt. 2.

\(^{72}\) See id.

\(^{73}\) Id. at r. 1.6 cmt. 4.

\(^{74}\) See infra text accompanying notes 76–80.

\(^{75}\) See supra Part I.

\(^{76}\) MODEL RULES OF PROF’L CONDUCT r. 1.6 (AM. BAR ASS’N 2016).

\(^{77}\) See supra text accompanying notes 21–24, 36–37.

\(^{78}\) See supra Part I.

\(^{79}\) MODEL RULES OF PROF’L CONDUCT r. 1.6 (AM. BAR ASS’N 2016).

continued . . .
client.\textsuperscript{80} Model Rule 1.18(a) defines who is a prospective client, while Model Rule 1.18(b) details an attorney’s duties to prospective clients who do not engage in a further attorney-client relationship. In relevant part, Model Rule 1.18(b) denotes that “a lawyer who had discussions with a prospective client shall not use or reveal information learned in the consultation . . . .”\textsuperscript{81} Model Rule 1.18 differs from Model Rule 1.6 in that it pertains to those who may not agree to have the attorney represent them, but instead merely sought a consultation or discussed the possibility of forming an attorney-client relationship.\textsuperscript{82} It also differs because in Model Rule 1.6 the ABA outlines the times when an attorney may or must reveal information relating to his or her representation of a client.\textsuperscript{83} However, no such allowance is made in Model Rule 1.18.\textsuperscript{84} While prospective clients should be protected, the ABA does distinguish the prospective from the actual client noting that “prospective clients should receive some but not all of the protection afforded clients.”\textsuperscript{85}

As the commentary to Model Rule 1.18 notes:

It is often necessary for a prospective client to reveal information to the lawyer during an initial consultation prior to the decision about formation of a client-lawyer relationship. The lawyer often must learn such information to determine whether there is a conflict of interest with an existing client and whether the matter is one that the lawyer is willing to undertake.\textsuperscript{86}

Just as Model Rule 1.6 protects client information in confidential meetings, so too does Model Rule 1.18 protect the information of a prospective client.\textsuperscript{87} The same analysis would then apply regarding whether having an A.I. system is allowed under the Model Rules.\textsuperscript{88} If a prospective client walks into an attorney’s office where an A.I. system is present, the attorney should either disclose that the system may potentially activate, or take steps to ensure that the device is not actively listening.\textsuperscript{89}

\textsuperscript{80} Id. at r. 1.18(a)-(b).
\textsuperscript{81} Id. at r. 1.18(b).
\textsuperscript{82} See id. at r. 1.6 cmt. 1; see also id. at r. 1.18(a).
\textsuperscript{83} Id. at r. 1.6(a)-(b).
\textsuperscript{84} See generally id. at r. 1.18 (making no mention of exceptions about revelation of prospective client materials in any subparts of the Rule).
\textsuperscript{85} Id. at r. 1.18 cmt. 1.
\textsuperscript{86} Id. at r. 1.18 cmt. 3.
\textsuperscript{87} Id. at r. 1.18(b).
\textsuperscript{88} Compare id. at r. 1.18(d)(2), with id. at r. 1.6(c).
\textsuperscript{89} Id. at r. 1.4(a) (requiring lawyers to disclose any circumstance regarding a continued . . .
Finally, Model Rule 5.3, which governs the behavior of non-lawyer assistants and indicates the responsibilities of attorneys in the non-lawyer’s supervision, is implicated. While Model Rule 5.3 clearly intended for this section to apply to human beings, it may help guide the decision of the attorney facing the ethical dilemma. Model Rule 5.3(b) directs that an attorney with supervisory authority over the non-lawyer assistant “shall make reasonable efforts to ensure that the person’s conduct is compatible with the professional obligations of the lawyer.” Model Rule 5.3(c) elaborates on when the lawyer is responsible for the non-lawyer’s failure to abide by the Model Rules, unambiguously noting that if the attorney fails to take remedial action when he or she is aware of the conduct and can mitigate or avoid the consequences of the failure then he or she is responsible for the non-lawyer’s actions.

While Model Rule 5.3 may apply to hired persons, it could eventually extend to A.I. assistants like Workspace Assistant or Siri. As A.I. systems become more complex and develop greater cognitive skills attorneys may be tempted to leverage these devices for legal research, automation, or predictive capabilities. Legal automation already occurs. For example, LegalZoom can generate form documents based on user input. Other services generate similar forms and have dramatically improved as more and more users become comfortable with the idea of online legal services. Meanwhile Workspace Assistant “can calculate time spent on specific matters,” as well as “answer questions relating to billable hours.” As these technologies progress, attorneys may begin to rely on them more frequently for easy form generation or convenience purposes, thus eliminating the need for

---

90 Id. at r. 5.3(c)(2).
91 See id. at r. 5.3(a).
92 Id. at r. 5.3(b).
93 Id. at r. 5.3(c)(2).
94 See generally id. at r. 5.3.
96 Id.
97 Id.
98 Id.

continued . . .
as many human resources. But then the question becomes, who is responsible when the automated form is incorrect, or an error occurs? Obviously, the attorney supervising should be held accountable, but does Model Rule 5.3 apply? As it stands, the Model Rules are silent on technology specific errors. Therefore, legal scholars should consider whether Model Rule 5.3 should extend to A.I. non-lawyer assistants before issues arise.

This is not to say that the Model Rules are averse to technology. In fact, the ABA updated the Model Rules in 2013 to include a requirement that attorneys stay competent by “keep[ing] abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology.” In the comment to Model Rule 1.6, the ABA clarifies that an attorney is not in violation of the rule if information is accessed without authorization or inadvertently disclosed if the attorney made reasonable efforts to prevent the unauthorized access or disclosure. The reasonableness of the efforts are assessed in a variety of ways, including:

- the sensitivity of the information,
- the likelihood of disclosure if additional safeguards are not employed,
- the cost of employing additional safeguards,
- the difficulty of implementing the safeguards, and
- the extent to which the safeguards adversely affect the lawyer’s ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).

The last portion of the comment specifically refers to technology, and suggests that the goal of keeping information secure is balanced by an attorney’s ability to take advantage of changing technologies. In other words, the ABA has no desire to make technologies so difficult to use that it renders such technology useless to an attorney. However,
the attorney must show the ABA that he or she has taken reasonable steps to ensure the technology keeps the client’s information secure in compliance with the actual language of Model Rule 1.6.\textsuperscript{108}

Consistent with the Model Rule’s comments on technology, some states have released Formal Ethics Opinions to supplement their own rules to be more technology friendly.\textsuperscript{109} For example, in 2010, the Florida Bar Association’s Formal Ethics Opinion 10-2 (Opinion 10-2) outlined in detail the steps Florida attorneys must take in order to secure client information on hard drive devices such as flash drives and personal digital assistants (PDA’s), which even just eight years later seem like outdated technologies.\textsuperscript{110} Opinion 10-2 created a four-step process for ensuring compliance with Florida Rules 4-1.1, 4-1.6(a), 4-5.3(b), the Florida state equivalent of Model Rules 1.1 (Competence), 1.6 (Confidentiality), and 5.3 (Duty to Supervise).\textsuperscript{111} These Florida measures included:

\begin{itemize}
  \item (1) identification of the potential threat to confidentiality along with the development and implementation of policies to address the potential threat to confidentiality;
  \item (2) inventory of the Devices that contain Hard Drives or other Storage Media;
  \item (3) supervision of nonlawyers to obtain adequate assurances that confidentiality will be maintained; and
  \item (4) responsibility for sanitization of the Device by requiring meaningful assurances from the vendor at the intake of the Device and confirmation or certification of the sanitization at the disposition of the Device.\textsuperscript{112}
\end{itemize}

The rationale for Opinion 10-2 was that many lawyers were “intentionally and unintentionally stor[ing] their clients’ information on these [d]evices.” in an attempt to keep up with growing use of technology in the workplace; therefore, the Florida Bar Board of Governors needed to supply the attorneys with guidance to avoid ethical

\textsuperscript{108} See id. at r. 1.6 cmt. 19.


\textsuperscript{111} Id.; MODEL RULES OF PROF’L CONDUCT r. 1.1, 1.6, 5.3 (AM. BAR ASS’N 2016).


\textit{continued . . .}
conflicts while also allowing the firms to change over time.  

Similarly, the State Bar of California Standing Committee on Professional Responsibility and Conduct (the Committee), which has not adopted the Model Rules, released a Formal Ethics Opinion on transmission of client data which could be susceptible to unauthorized access by third parties (California Opinion).  Describing technology as an “indispensable tool of law,” the Committee created a hypothetical in which a new Associate first takes his work computer to a local coffee shop where he researches and sends emails to the client over a public wireless network.  Then the Associate travels home with the laptop where he accessed client files on his personal wireless network in order to complete a project and continue to communicate via email to his client.  In today’s busy world, taking a work laptop home or to lunch to continue working after hours is not uncommon.  However, as the Committee noted, without appropriate safe guards, a public wireless network or an unsecured network can easily be accessed by others who are not privy to private communications.  In order to assess whether the Associate is subject to discipline under California’s Ethical Rules, the Committee set up a six-part test to determine whether the use of technology constitutes a violation of confidentiality or competence.  Those six steps included:

(1) the level of security attendant to the use of that technology, including whether reasonable precautions may be taken when using the technology to increase the level of security; (2) the legal ramifications to a third party who intercepts, accesses or exceeds authorized use of the electronic information; (3) the degree of sensitivity of the information; (4) the possible impact on

---

113 Id.
115 Id.
116 Id.
118 Id.
119 Id.
the client of an inadvertent disclosure of privileged or confidential information or work product; (5) the urgency of the situation; and (6) the client’s instructions and circumstances, such as access by others to the client’s devices and communications.\textsuperscript{120}

Under these standards, the associate risks breaching his client’s confidentiality at the coffee shop because the public network was not secure.\textsuperscript{121} However, the Committee, recognizing that working in a coffee shop is not uncommon, noted that the Associate could take additional steps such as “using a combination of file encryption, encryption of wireless transmissions and a personal firewall.”\textsuperscript{122} The Committee even suggested that, depending on the sensitivity of the matter, the attorney’s extra steps in protecting the information may not be enough.\textsuperscript{123} The Committee had similar feelings regarding the attorney’s personal wireless network, but it felt that working on the matter at home over a private network was less concerning than working on a client matter in public.\textsuperscript{124}

The California Opinion and Opinion 10-2 highlight the state bar associations’ understanding that technology needs to be in the workplace.\textsuperscript{125} But these opinions also emphasize the importance of attorney supervision and understanding of the technologies which they are utilizing.\textsuperscript{126} While these opinions cover technologies which are seemingly out of date, the standards they set forth to determine the reasonable steps an attorney may take can be applied to technologies like Alexa.\textsuperscript{127} By identifying the Model Rules which may presently conflict with allowing technologies like Alexa or Workspace Assistant in the workplace attorneys, the ABA, attorneys, and tech companies can work together to ensure that client information is protected and attorneys are not at risk of an ethical violation while staying current with technological trends. Part III below suggests how the standards from the Model Rule Comment 1.6, Opinion 10-2, and the California Opinion might be applied to A.I. systems like Alexa and Workspace Assistant.\textsuperscript{128} Part III will also suggest precautions which attorneys and firms may

\textsuperscript{120} Id. at 1.
\textsuperscript{121} Id. at 7.
\textsuperscript{122} Id.
\textsuperscript{123} Id.
\textsuperscript{124} Id.
\textsuperscript{126} Id.
\textsuperscript{127} Id.
\textsuperscript{128} See infra Part III.  

\textit{continued . . .}
initiate on their own to bring clients peace of mind while also allowing these A.I. systems to assist attorneys.\textsuperscript{129}

**IV. Ethical Technology and the Evolving Workplace**

Looking to Model Rule 1.6 comment eighteen (Comment Eighteen), the factors listed in Part II play a critical role in assessing whether the attorney has violated his or her ethical duty.\textsuperscript{130} Of particular importance to the ethical dilemma of whether or not an A.I. assistant violates the Model Rules is the cost of employing additional safeguards, the difficulty of implementing those safeguards, and the likelihood of disclosure.\textsuperscript{131} A.I. systems like Alexa or Google Home are managed largely by the platform which owns the technology.\textsuperscript{132} Meanwhile a system like Workspace Assistant’s billable hours feature on Alexa runs within the Reuters Elite 3E secure platform, and is protected behind the specific law firm’s firewalls with little interaction with Amazon other than leveraging the ASR capabilities of the device.\textsuperscript{133}

Applying Comment Eighteen’s test to the two A.I. assistants helps distinguish which system would be allowed under the existing rule and which would require further analysis.\textsuperscript{134} For a regular Alexa there are almost no safeguards, merely Amazon’s privacy policy which only governs how the device may be used and what information Amazon itself may be privy to.\textsuperscript{135} The likelihood of disclosure is also a concern given that Amazon is able to store recorded data in the cloud, which can then be subpoenaed.\textsuperscript{136} More importantly more research has shown that Alexa, like practically all connected devices, can indeed be hacked.\textsuperscript{137}

\textsuperscript{129} See infra Part III.

\textsuperscript{130} See supra Part II.

\textsuperscript{131} MODEL RULES OF PROF’L CONDUCT r. 1.6 cmt. 18 (AM. BAR ASS’N 2016).


\textsuperscript{134} MODEL RULES OF PROF’L CONDUCT r. 1.6 cmt. 18.


\textsuperscript{136} See Lohr, supra note 36.

Thus, a normal Alexa run by the Amazon platform has already failed two of the three important elements in Comment Eighteen.  

On the other side of the spectrum is Workspace Assistant, which uses Alexa but is not run on the Amazon platform. Workspace Assistant, which is the application that allows Alexa to record billable hour information, uses a platform called Elite Workspace designed by Thomas Reuters, which operates as a business management platform for law firms. Elite Workspace, including the Workspace Assistant, works within the firm’s existing security walls, thus addressing the issue of disclosure and addressing the difficulty of implementing safeguards to ensure the information does not leak. The Elite Workspace platform does require firms to purchase the platform thereby addressing the third prong of Comment Eighteen’s main concerns, which is the cost of implementation. While specific costs were not available to the author, the platform is priced to sell. Meanwhile Workspace Assistant is free if Elite Workspace has already been purchased, so there is no added cost to the user.

What is unclear with Workspace Assistant is whether it must be constantly running for the billable hours to be tracked. If Workspace Assistant is on, does this mean Alexa is actively listening? For example, if an attorney said “Alexa, track hours for client matter 1234-77” presumably this would activate the Workspace Assistant feature that would begin timing. The problem is that if Workspace Assistant is actively running, this may also mean that Alexa is recording because it is actively listening. Therefore, if a client is in the room with the attorney or if the attorney is on the phone, those conversations may be recorded because the device is still “a low touch into the Amazon

---

138 See supra Part II.
141 Ambrogi, supra note 42.
142 See supra Part II.
143 See Ambrogi, supra note 42.
145 See id.
146 See Li, supra note 99.
147 Ambrogi, supra note 42.

continued . . .
environment."


To ensure Workspace Assistant does not violate the Model Rule 1.6, when an attorney begins billable hours within the platform he or she should either gain written informed consent from the client per Model Rule 1.6(a), or the device should be unplugged before any oral communication regarding the client’s representation begins. Following the conversation, the attorney should manually input the time in which the conversation took place, unless written informed consent from the client has been granted. To attain informed consent, the attorney should advise the client of the Workspace Assistant’s presence, inform the client exactly what will be recorded, and inform the client of his or her right to confidentiality.

Regarding potential clients under Model Rule 1.18, Workspace Assistant should be turned off to avoid any confusion. Since no client matter number would exist there is no reason to have Workspace Assistant on. If the firm requires the attorney to bill hours relating to potential client meetings, the attorney may manually input those hours. This will avoid unnecessary potential client confusion and ensure the attorney’s compliance with the Model Rules.

B. Recommendation 2: Platforms Like Amazon and Google Could Develop Secure Cloud Space.

Much like Reuters has developed a secure network to house Workspace Assistant data, it would behoove platforms like Amazon and Google to develop a business friendly cloud space that could be encrypted. Amazon has already developed Alexa for Business, which is capable of performing tasks such as alerting the information technology department to a technical issue, controlling conference room equipment, and even providing the latest company sales data. Alexa

---

148 Id.
149 See Model Rules of Prof’l Conduct r. 1.6(c) (Am. Bar Ass’n 2016).
150 Id.
151 See Model Rules of Prof’l Conduct r. 1.18.
152 Id.
154 Jason Hilner, Cheat Sheet: Alexa for Business, TechRepublic (Dec. 1, continued . . .
for Business is compatible with multiple applications including WebEx, Microsoft Office 365, and Polycom, but it does not seem to offer a secure cloud storage space for all of the information Alexa is retrieving.\textsuperscript{155} So while an employee has the ability to customize his or her Alexa work experience with his or her personal preferences, he or she is unable to secure his or her data in an encrypted space.\textsuperscript{156} Therefore, before a firm decides to invest in Alexa for Business, it would be beneficial for Amazon to develop a platform that secures all of the stored data collected around the office, from client phone calls recorded by the Alexa in the hallway to recorded conferences occurring via Alexa enabled WebEx.\textsuperscript{157} These encrypted clouds may be able to operate within the firm’s existing firewalls, or they could be an entirely separate cloud space, which would allow attorneys to still have an Alexa with the peace of mind in knowing that they have taken steps to secure the data by applying additional safe guards with little difficulty in compliance with Comment Eighteen.

C. Recommendation 3: Be Aware and Be Open with the Client.

Firms can look to Opinion 10-2, the California Opinion, or their own state ethics opinions to determine how technology compliance with the state Rules is assessed by their state bar.\textsuperscript{158} In reviewing Opinion 10-2, identifying the technology that may result in unauthorized access, keeping an inventory of the technology used in the space, providing adequate supervision of staff and other non-lawyers utilizing the technology, disposing of the device properly when no longer in use, and certifying that the device has properly been wiped are all steps attorneys can take to proactively ensure that they are in compliance with the Rules of Professional Conduct.\textsuperscript{159} In order to identify the technology and understand how it should properly be monitored and disposed of, attorneys need to be aware of how the technology actually works.\textsuperscript{160}

\begin{thebibliography}{9}
\bibitem{Id} Id.
\bibitem{Id} Id.
\bibitem{Id} See MODEL RULES OF PROF’L CONDUCT r. 1.1 cmt. 8 (AM. BAR ASS’N 2016) (noting an attorney should understand the “risks and benefits of the technology”).
\end{thebibliography}

continued . . .
Without a thorough understanding of such technology it is impossible for the attorney to adequately inform the client of the device’s presence and the risks and benefits associated with utilizing the device; therefore, the client cannot give his or her informed consent to the device’s use regarding the client’s representation, which is a violation of Model Rule 1.6(a).  

As it stands, an attorney would need to get informed consent by every client or potential client should a regular Alexa system be installed and in use in the office space by either the attorney or those under the supervision of the attorney. A normal Alexa system has a low level of security; unless the attorney is using Workspace Assistant, he or she has not taken any additional steps to increase the level of security. Furthermore, the legal ramifications to the third party who intercepts the information housed in the Alexa cloud (e.g., Amazon) are still unclear. An attorney needs to be able to assess the level of security associated with the technology and analyze the possible impact on the client should the information recorded and saved in the Alexa cloud space be released or accessed without authorization. As is the case with most situations, a client’s instructions also matter, but the client cannot give instructions regarding the device’s use if he or she is not made aware of its presence. In sum, unless an attorney, or a staff member, using an Alexa ensures that the device is not recording by unplugging the device during relevant oral communications including, phone calls, in person meetings, or staff meetings regarding the client matter, the client should be made aware of the device’s presence and the risks and benefits associated with it. After a client has been

---

163 Id.
164 In one case, a defendant, in conjunction with Amazon, agreed to release Alexa Data to Prosecutors in a murder trial. Previously Amazon had fought the Court order to release the Alexa recordings, but no Court decision was rendered because Defendant voluntarily released the information.) See Andrew Blake, Amazon Gives Up Alexa Data Sought in Murder Probe, THE WASHINGTON TIMES (Mar. 8, 2017), https://www.washingtontimes.com/news/2017/mar/8/amazon-gives-alexa-data-sought-murder-probe/.
166 Id.
adequately informed, the attorney should get the client to sign a
document stating that he or she is aware of the device and, after being
adequately appraised of his or her rights, gives his or her informed
consent to the device’s use.\(^\text{168}\)

V. CONCLUSION

As technology proceeds to develop at a rapid pace, attorneys are
tasked with ensuring they keep up with the latest innovations.\(^\text{169}\)
However, they cannot forsake a client’s confidentiality or risk a client’s
information later being leveraged against them because the attorney or
a staff member was unaware that his or her weak A.I. system was
recording and storing that information.\(^\text{170}\) By working closely with
technology developers to create secure cloud storage space, providing
continuing legal education centered around how these devices can be
used properly in an office space, and adequately informing clients of
their rights, attorneys can and should leverage new A.I. technology to
become faster, more efficient, and more cost effective in their
businesses.

\(^{168}\) See MODEL RULES OF PROF’L CONDUCT r. 1.6, 1.18 (AM. BAR ASS’N 2016).
\(^{169}\) See MODEL RULES OF PROF’L CONDUCT 1.1 cmt. 8.
\(^{170}\) See MODEL RULES OF PROF’L CONDUCT 1.6, 1.18, 5.3.