VIRGINIA JOURNAL OF LAW & TECHNOLOGY

SPRING 2021 UNIVERSITY OF VIRGINIA VOL. 24, NOTE 2

# It's Smart, but Is It Ethical? Confidentiality in an Environment That Is Listening

ARMINA MANNING†



† J.D., University of Virginia School of Law (2021); B.A., College of William & Mary (**YYYY**). Acknowledgments and gratitude to Professor George Cohen for his guidance through the early stages of this paper, and to Professor Gregory Mitchell for his notes and advice.

## ABSTRACT

This paper examines the confidentiality implications of cloud-connected voice-computing technology. The ubiquity of this technology results in the possibility of being under surveillance at any given time by a device known to transmit audio from its environment to be saved on cloud servers. Part I describes the risks and benefits presented by this technology, Part II examines existing guidance on what the duty of confidentiality requires, Part III A offers examples of reasonable measures that lawyers may take to safeguard client confidentiality around cloud-connected voice-computing devices, and Part III B pulls everything together through the analysis of four hypothetical situations. In Part IV, a brief conclusion outlines the need for more specific guidance on how the presence of cloud-connected voice-computing technology must modify the behavior of modern lawyers.

# TABLE OF CONTENTS

## INTRODUCTION

"Yes, the retail development across from the Lexus dealership—he plans to put in an offer on Monday. We're hoping they take $1.2 million, but he'll go up to $1.5." An attorney working from home may have a conversation such as this, discussing confidential client information. This attorney's office door is open, and the Alexa in her living room hears "Lexus" and begins to record. After recording about 15 seconds of audio, the Alexa isn't sure if there was a command. Meanwhile, a recording of the audio is queued for human review to help improve Alexa's voice services. Depending on other information that Amazon already has about the attorney's location, a human agent of Amazon may now have access to confidential client information about a parcel of land that the attorney's client hopes to buy.

Due to the rising prevalence of smart home devices[1] and personal assistants in smartphones and speakers,[2] a person who is up to date with technology should reasonably expect the

---

[1] The ownership and use of voice-computing cloud-connected devices is higher than ever:

> According to a January 2020 report from NPR and Edison, 60 million people (or 24 percent of adults 18 and over) in the US own at least one smart speaker device at the end of 2019. However, with a total number of 157 million smart speakers out in the wild, that's 2.6 smart speaker devices per household. The report also concluded that 69 percent of smart speaker owners use their device daily. That's a lot of conversations potentially being listened to without your knowledge.

Joanna Nelius, *Unplug Your Smart Speakers While You're Working From Home*, GIZMODO (Mar. 23, 2020), https://gizmodo.com/unplug-your-smart-speakers-while-youre-working-from-hom-1842455162; *see also* Geoffrey Fowler, *You watch TV. Your TV watches back.*, WASH. POST (Sept. 18, 2019), https://www.washingtonpost.com/technology/2019/09/18/you-watch-tv-your-tv-watches-back/.

[2] The best examples are always-listening digital assistants and home surveillance devices like Google's Home Assistant and Nest Hub, Amazon's Alexa and Ring, Apple's HomePod and Siri, Microsoft's Cortana, and Samsung's Bixby, among others.

possibility of being under surveillance at any given time.[3] This technology is here to stay; therefore, lawyers must not view the idea of complying with the Model Rules of Professional Conduct in a world of constant surveillance as an outlier situation. Since the constant possibility of surveillance is reality, it is necessary to be clear-eyed and well-armed with knowledge about how to meet one's ethical obligations.

Of particular note to lawyers is the advent of "voice computing."[4] It is commonly understood that face-to-face discussion is the best way to preserve the privacy of sensitive communications.[5] Now the spoken word has instead become "the universal remote to reality,"[6] allowing people to control technology just as they would with a keyboard and screen. However, voice computing is far more imprecise than keyboard inputs, and may easily result in recorded data that was not intended as an input.[7] The threat that this type of computing poses to the confidentiality of even face-to-face communications is clear: when there is a voice-computing

---

[3] *See* Adam Clark Estes, *The Terrible Truth About Alexa*, GIZMODO (Apr. 27, 2019), https://gizmodo.com/the-terrible-truth-about-alexa-1834075404 ("In a future where internet-connected microphones are present in an ever-increasing number of rooms, a system like this could always be listening.").

[4] JAMES VLAHOS, TALK TO ME: HOW VOICE COMPUTING WILL TRANSFORM THE WAY WE LIVE, WORK, AND THINK 3 (2019).

[5] In his discussion of privacy in the Fourth Amendment context, Schulhofer comments that the only sure way to avoid exposing information "voluntarily" is to, "conduct all confidential communications face-to-face". This illustrates a common understanding that other forms of communication inevitably involve the capture of information. STEPHEN J. SCHULHOFER, MORE ESSENTIAL THAN EVER: THE FOURTH AMENDMENT IN THE TWENTY FIRST CENTURY 131 (2012).

[6] VLAHOS, *supra* note 4, at 3.

[7] *See* Daniel J. Dubois, Roman Kolcun, Anna Maria Mandalari, Muhammad Talha Paracha, David Choffnes & Hamed Haddadi, *When Speakers Are All Ears: Understanding When Smart Speakers Mistakenly Record Conversations*, MON(IOT)R RESEARCH GROUP (last updated July 21, 2020), https://moniotrlab.ccis.neu.edu/smart-speakers-study/ [hereinafter MON(IOT)R RESEARCH GROUP]; Jay Stanley, *The Privacy Threat From Always-On Microphones Like the Amazon Echo*, ACLU (Jan. 13, 2017), https://www.aclu.org/blog/privacy-technology/privacy-threat-always-microphones-amazon-echo.

cloud-connected device in the room, the security of face-to-face communication is undermined.[8]

This paper seeks to explore the ethical implications for lawyers of using certain IOT[9] or "smart" devices in their practice, with a focus on the duty of confidentiality. The privacy implications of these devices have been thoroughly discussed in both the consumer privacy and Fourth Amendment contexts, but few scholars have discussed the ethical implications.[10] Most of the discussions on point tend to appear in the form of professional commentary, such as blog posts,[11] articles published for an intended audience of other practitioners,[12] or articles published on a private enterprise's

---

[8] *See* Ryan Morrison, *Alexa IS listening to you: Former Amazon Executive Reveals He Switches OFF His Smart Speaker Whenever He Wants a 'Private Moment'*, DAILY MAIL (Feb. 17, 2020), https://www.dailymail.co.uk/sciencetech/article-8013225/Former-Amazon-Executive-reveals-switches-Alexa-wants-private-moment.html.

[9] IOT or "Internet of Things" describes "the networking capability that allows information to be sent to and received from objects and devices (such as fixtures and kitchen appliances) using the Internet." *Internet of Things*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/Internet%20of%20Things (last visited Feb. 27, 2020).

[10] *See* Myles G. Taylor, *Seeing Clearly? Interpreting Model Rule 1.6(c) for Attorney Use of Cloud Computing Technology*, 45 MCGEORGE L. REV. 835 (2014); Jan L. Jacobowitz & Justin Ortiz, *Happy Birthday Siri! Dialing in Legal Ethics for Artificial Intelligence, Smartphones, and Real Time Lawyers*, 4 TEX. A&M J. PROP. L. 407 (2018).

[11] *See, e.g.*, Peggy Wojkowski, *Alexa, Am I Violating Legal Ethics?*, ON THE EDGES OF SCIENCE AND LAW (May 31, 2017), http://blogs.kentlaw.iit.edu/islat/2017/05/31/alexa-violating-legal-ethics/.

[12] *See, e.g.*, Nicole Black, *Speech-to-Text Dictation: A 21st-Century Twist to a Traditional Law Firm Tool*, ABA J. (Aug. 23, 2019), https://www.abajournal.com/web/article/speech-to-text-dictation-a-21st-century-twist-to-a-traditional-law-firm-tool; Daniel E. Harmon, *Vulnerable Connections: Legal Analysts Consider Privacy, Security & the IOT*, 32 NO. 17 LAW. PC 1 (June 1, 2014); Christopher Riordan, *Digital Billing Assistants and Professional Responsibility*, LAW TECHNOLOGY TODAY (Feb. 27, 2018), https://www.lawtechnologytoday.org/2018/02/digital-billing-assistants/; Gordon D. Cruse, *The Trouble with Devices and the Data They Contain*, 41-WRT FAM. ADVOC. 33 (2019).

webpage as a display of expertise.[13] Thus, there is a need for a more sustained, scholarly treatment of the problem. This paper responds to the gap in scholarship by examining the lawyer's duty of confidentiality in light of devices that automatically record audio for cloud processing or storage.[14]

Part I describes the technology at issue in more detail, outlining the risks and benefits presented by cloud-connected voice-computing devices. Part II discusses what confidentiality rules require by examining the Model Rules of Professional Conduct, formal opinions by the ABA Standing Committee on Ethics and Professional Conduct, and principles articulated by the Restatement, Third, of The Law Governing Lawyers. Part III introduces examples of reasonable measures that a lawyer may take to adhere to her ethical obligations, and then walks through hypothetical scenarios relevant to lawyers using available ABA guidance. Finally, Part IV offers concluding remarks.

---

[13] *See, e.g.*, Sharon D. Nelson & John W. Simek, *Are Alexa and Her Friends Safe to Use in Your Law Office? The Pros and Cons of Personal Assistants*, SENSEI ENTERPRISES, INC. (Aug. 29, 2017), https://senseient.com/articles/alexa-friends-safe-use-law-office-pros-cons-personal-assistants/; Gaby Isturiz, *What All Law Firms Need to Know About Siri*, ADERANT (June 25, 2015), http://blog.bellefield.com/what-all-law-firms-need-to-know-about-siri.

[14] A note on jargon: this paper uses the terms "cloud computing," "voice computing," "IOT" ("internet of things"), and "digital assistant" to refer to the devices discussed. These terms are not synonymous; however, they all refer to various aspects of the devices concerned herein. This paper focuses on voice *and* cloud computing devices. Many of the devices concerned may be known as "digital assistants," "smart speakers," or "smart homes," but note that the same capabilities are often found in smartphones as well.

## I. PART ONE

The technologies within the scope of this work have two main attributes: voice computing and cloud processing. Voice-computing technology is equipped to interact with a user through the use of voice commands; therefore, the device necessarily includes a microphone and some method of processing verbal inputs. Cloud processing means that the device is connected with an outside system, generally over the internet, that receives data collected by the device and processes the data elsewhere.

In order to better understand cloud-connected voice-computing technologies, the following subparts outline the risks and benefits presented by these devices.

### A. The Risks Presented by Voice Computing and Cloud Computing

The technology which implicates new confidentiality concerns is not the entirety of cloud computing.[15] The specific area of concern is voice-computing smart devices that fall under the cloud computing umbrella by virtue of sending the data they collect elsewhere for processing. Neither cloud computing nor voice computing alone raise alarm, but their combination gives rise to scenarios wherein the information sent to the cloud is a snippet of audio that is processed, transcribed, and perhaps reviewed by human employees.[16] The

---

[15] Cloud computing denotes services (such as email, storage, and document editing) that are controlled by third parties and accessed over the internet. ABA Comm'n on Ethics 20/20 Issues Paper Concerning Client Confidentiality and Lawyers' Use of Technology (Sept. 20, 2010), https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/2011build/ethics2020/clientconfidentiality_issuespaper.pdf

[16] *See* Geoffrey A. Fowler, *Alexa Has Been Eavesdropping on You This Whole Time*, WASH. POST (May 6, 2019), https://www.washingtonpost.com/technology/2019/05/06/alexa-has-been-eavesdropping-you-this-whole-time/ ("Amazon employees listen to recordings to train its artificial intelligence. Amazon acknowledged that some of those employees also have access to location information for the devices that made the recordings."); *see also* Matt Day, Giles Turner &

significance of the fact that data is available as a snippet of audio cannot be overstated, as it is this precise method of data collection and storage that presents information "in an instantly comprehensible form (oral speech)"[17] to any who come across it.

Digital assistant devices like the Amazon Echo, Google Home, and Apple HomePod are listening all the time, but most of that material is not saved and catalogued.[18] It would be a

---

Natalia Drozdiak, *Amazon Workers Are Listening to What You Tell Alexa*, BLOOMBERG (Apr. 10, 2019), https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio (reporting on the human role in Alexa's voice review process, and also the use of human employees to manually identify vehicles and people captured in videos by Amazon-owned Ring doorbell cameras.); *see also* James Vlahos, *Smart Talking: Are Our Devices Threatening Our Privacy?*, GUARDIAN (Mar. 26, 2019), https://www.theguardian.com/technology/2019/mar/26/smart-talking-are-our-devices-threatening-our-privacy ("[T]he review process can also be shockingly intimate. . . . employees showed me how they received daily emails listing recent interchanges between people and one of the company's chat apps. The employees opened one such email and clicked on a play icon. In clear digital audio, I heard the recorded voice of a child . . . ."); *see also* Graham Johnson, *Privacy and the Internet of Things: Why Changing Expectations Demand Heightened Standards*, 11 WASH. U. JURIS. REV. 345, 355–56 (2019) ("Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of Voice Recognition.").

[17] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 99-413 (Mar. 10, 1999) (referencing the risk posed by cell phone signal interception as compared with other methods of communication).

[18] *Data Security and Privacy on Devices That Work with Assistant*, GOOGLE NEST HELP, https://support.google.com/googlenest/answer/7072285?hl=en (last visited Mar. 13, 2020) ("Is my Google Nest device recording all of my conversations? No. [...]"; "[t]he Google Assistant is designed to wait in standby mode until it is activated, like when you say 'Hey Google.' [...] In standby mode, it processes short snippets of audio (a few seconds) to detect an activation (such as 'Ok Google'). If no activation is detected, then those audio snippets won't be sent or saved to Google. When an activation is detected, the Assistant comes out of standby mode to fulfill your request." ); *Alexa and Alexa Device FAQs*, AMAZON HELP & CUSTOMER SERVICE, https://www.amazon.com/gp/help/customer/display.html?nodeId=201602230 (last visited Mar. 13, 2020) ("Is Alexa recording all my conversations?

gross overstatement to imply that these devices record and store every conversation within earshot.[19] Instead, they listen for a "wake word" that notifies the always-listening device that the user now intends to interact with the device; for the Amazon Echo, the word may be "Alexa" or "Echo," and for Google's Assistant, it may be "Hey, Google" or "Ok, Google."[20] After the wake word is uttered, the interaction is recorded and processed offsite in the cloud, and in some cases is reviewed by a human.[21] Voice-computing technology is constantly improving, but is still imperfect.[22] It's not uncommon for digital assistants to register a false positive; that is, "pick up a sound from the TV, or a stray bit of conversation that sounds enough like one of their wake words," and start

---

No. By default, Echo devices are designed to detect only your chosen wake word (Alexa, Amazon, Computer or Echo).").

[19] "Are these devices constantly recording our conversations? In short, we found no evidence to support this. The devices do wake up frequently, but often for short intervals (with some exceptions)." MON(IOT)R RESEARCH GROUP, *supra* note 7.

[20] *Id.*

[21] Tom McKay, *Amazon's Human Helpers Are Quietly Listening in on Some Alexa Recordings*, GIZMODO (Apr. 10, 2019), https://gizmodo.com/amazons-human-helpers-are-quietly-listening-in-on-some-1833960052; Nick Statt, *Google Defends Letting Human Workers Listen to Assistant Voice Conversations*, VERGE (July 11, 2019), https://www.theverge.com/2019/7/11/20691021/google-assistant-ai-training-controversy-human-workers-listening-privacy; David Monsees, *More Information About Our Processes to Safeguard Speech Data*, GOOGLE: THE KEYWORD (July 11, 2019), https://www.blog.google/products/assistant/more-information-about-our-processes-safeguard-speech-data/; *Improving Siri's Privacy Protections*, APPLE STATEMENT (Aug. 28, 2019) (apologizing for how Apple had handled human review of audio for Siri), https://www.apple.com/newsroom/2019/08/improving-siris-privacy-protections/ .

[22] *See* Kellen Gillespie, Ioannis C. Konstantakopoulos, Xingzhi Guo, Vishal Thanvantri Vasudevan & Abhinav Sethy, *Improving Device Directedness Classification of Utterances with Semantic Lexical Features*, 2020 IEEE INT'L CONF. ACOUSTICS, SPEECH & SIGNAL PROCESSING 7859 (May 2020), https://assets.amazon.science/a9/12/18a83a58403895e386685e4226cb/scipub-1236.pdf.

recording.[23] Across the range of digital assistant devices, recent testing by researchers at Northeastern University and Imperial College London has shown that smart speakers may activate in error between 1.5 to 19 times per day.[24] A later study observed

---

[23] John Kruzel, *Is Your Amazon Alexa Spying on You?*, POLITIFACT (May 31, 2018), https://www.politifact.com/factchecks/2018/may/31/ro-khanna/your-amazon-alexa-spying-you/. Journalist Adam Estes recalls the experience of reviewing his own digital assistant's voice command records:

> The extent to which false positives are a problem became glaringly evident the moment I started reading through my history of Alexa commands on Amazon's website. Most of the entries are dull: "Hey Alexa;" "Show me an omelet recipe;" "What's up?" But sprinkled amongst the mundane dribble was also a daunting series of messages that said, "Text not available—audio was not intended for Alexa." Every time I saw it, I saw it twice again and read it aloud in my head: "Audio was not intended for Alexa." These are the things Alexa heard that it should not have heard, commands that have been sent to Amazon's servers and sent back because the machine decided the wake word had not been said or that Alexa had recorded audio when the user wasn't giving a command. In other words, they're errors.

Estes, *supra* note 3.

[24] The research conducted by Northeastern and the Imperial College is ongoing; last updated on February 14, 2020, with indications that further updates are forthcoming. The researchers tested for false activations by playing audio of television shows for different types of smart speakers.

> Everything described below is based on activations when the wake word was not spoken. . . . Are activations long enough to record sensitive audio from the environment? Yes, we have found several cases of long activations: 10% of the activations were at least 10 seconds long for the Homepod, 9 seconds for Google Home Mini, and 8 seconds for Echo Dot 2nd generation with "Echo" wake word. Half of the activations for Homepod and Echo Dot 2nd generation (Alexa and Computer wake words) were also at least 4 seconds long. During our experiments, we have also seen rare cases of activations lasting up to 43 seconds; however, such cases – which also appeared in our

about 0.95 misactivations per hour of audio, or 1.43 misactivations per 10,000 words spoken.[25] In this way, a device that is functioning correctly can record, save, and transmit audio that a user does not intend to direct to the device.[26] Of course, a device that is not functioning correctly might do far more.[27] Moreover, it can be difficult to learn how companies plan to use and protect any information that their devices collect.[28]

While such devices are capable of recording our utterances without our contemporaneous knowledge, an important detail is that these devices involve human review of some of those recordings *by design*.[29] That means that users of

---

> preliminary findings – represent situations that only happened in a single experiment, and therefore we have decided to consider them as outliers.

MON(IOT)R RESEARCH GROUP, *supra* note 7 (emphasis removed).

[25] MON(IOT)R RESEARCH GROUP, *supra* note 7.

[26] "One journalist, writing about virtual assistants, shared her personal discovery: 'I was surprised when I checked my Amazon Echo recordings. In one recording, I was explaining why I wasn't taking a deal on a commercial building that I had for sale.'" Jacobowitz & Ortiz, *supra* note 10, at 422.

[27] On October 4, 2017, journalists who attended the Google Home Mini product unveiling were gifted devices as event swag. It was later found that the devices handed out at the event suffered from a hardware flaw that triggered near constant recording, instead of recording only upon use of the wake word. Taylor Hatmaker, *A Messed Up Google Home Mini Recorded a Tech Reporter 24/7*, TECHCRUNCH (Oct. 10, 2017), https://techcrunch.com/2017/10/10/google-home-mini-recorded-24-7-androidpolice/.

[28] Johnson, *supra* note 16, at 354–56 (commenting on the difficulty of locating relevant privacy policies, and the confusing language found within the policies).

[29] David Monsees, *More Information About Our Processes to Safeguard Speech Data*, GOOGLE: THE KEYWORD (July 11, 2019), https://www.blog.google/products/assistant/more-information-about-our-processes-safeguard-speech-data/. Note that Amazon now claims to allow users to opt out of human review of their Alexa recordings. This change in policy was implemented in the summer of 2019, when Google, Apple, and Amazon were all subject to pressure by the European Union over human review of digital assistant recordings. Google and Apple temporarily halted human review at that time, while Amazon provided the opt-out option. Alex

these devices should be on notice of the chance that their utterances could be disclosed to other humans, not as a result of hacking, but in the regular course of business.[30]

### B. The Benefits of Voice Computing and Cloud Computing in Legal Practice

There are many practical uses for voice-computing, cloud-connected devices in legal practices. A lawyer can retrieve information from her phone, place a call without dialing or send an email without typing, leave herself a voice note, and more.[31] Lawyers are known to use digital assistants in the office for reminders, alarms, and timekeeping.[32] Some digital assistants can integrate with email to read messages aloud and delete them upon a voice command, or be used to

---

Hern, *Alexa Users Can Now Disable Human Review of Voice Recordings*, GUARDIAN (Aug. 5, 2019), https://www.theguardian.com/technology/2019/aug/05/alexa-allows-users-to-disable-human-review-of-voice-recordings.

[30] This work does not focus on security vulnerabilities and hacking/phishing, but note that security breaches remain a huge concern. *See, e.g.*, Dan Goodin, *Alexa and Google Home Abused to Eavesdrop and Phish Passwords*, ARS TECHNICA (Oct. 20, 2019), https://arstechnica.com/information-technology/2019/10/alexa-and-google-home-abused-to-eavesdrop-and-phish-passwords/; *see also* Lily Hay Newman, *Turning an Echo Into a Spy Device Only Took Some Clever Coding*, WIRED (Apr. 25, 2018), https://www.wired.com/story/amazon-echo-alexa-skill-spying/.

[31] FindLaw Attorney Writers, *How Lawyers Can Use Siri and Other Personal Assistant Voice Apps*, FINDLAW (last updated June 20, 2016), https://technology.findlaw.com/mobile/how-lawyers-can-use-siri-and-other-personal-assistant-voice-apps.html.

[32] Dennis Kennedy, Alexander Paykin & Greg Siskind, *How Do You Use Your Digital Assistant?*, LAW TECHNOLOGY TODAY (May 30, 2018), https://www.lawtechnologytoday.org/2018/05/digitial-assistants/; *see also* William Vogeler, *Google Assistant Is Ready to Assist Your Law Practice*, FINDLAW (June 14, 2017), https://blogs.findlaw.com/technologist/2017/06/google-assistant-is-ready-to-assist-your-law-practice.html.

start previously scheduled phone or video calls by voice command.[33] Relegating these time management, recordkeeping, and logistical tasks to a machine helps reduce costs and free up the time of lawyers and support staff. For some solo practitioners, the help of such a device may even obviate the need for support staff. Further, cloud processing adds value to voice-computing digital assistants by facilitating improved speech recognition, and therefore improved 'digital assisting' over time.[34]

In order to better understand how and when lawyers may use these powerful devices to assist in their practices, the next part examines and summarizes existing rules and guidance relevant to the confidentiality implications of various technologies.

## II. PART TWO

The American Bar Association's Model Rules of Professional Conduct are a set of rules and commentaries on the ethical and professional responsibilities of licensed attorneys. Although the Model Rules are not themselves binding, all fifty states and the District of Columbia have adopted legal ethics rules based at least in part on the Model Rules.[35] Over time, the ABA has also released advisory ethics opinions to clarify specific issues that the Model Rules may not address fully. Together, these sources supply the basis for

---

[33] Mark Rosch, *Do Virtual Assistants Like Alexa and Google Assistant Have a Place in the Office*, INTERNET FOR LAWYERS (Jan. 9, 2018), https://www.netforlawyers.com/content/smart-home-office-amazon-echo-alexa-google-home-assistant-206.

[34] Day, Turner & Drozdiak, *supra* note 16 (noting that at Amazon, this information helps train "speech recognition and natural language understanding systems, so Alexa can better understand your requests"; similarly, "[a]t Google, some reviewers can access audio snippets from its Assistant to help train and improve the product . . . .").

[35] *Alphabetical List of Jurisdictions Adopting Model Rules*, ABA (Mar. 28, 2018), https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/alpha_list_state_adopting_model_rules/.

defining lawyers' professional and ethical responsibilities. The American Law Institute also publishes a restatement of the Law Governing Lawyers, which covers this material and may aid in interpretation. The following sections, A, B, and C, examine each source and identify gaps and uncertainties in the current guidance.

### A. The Model Rules of Professional Conduct

The ABA began to examine and address issues related to cloud computing when it established the ABA Commission on Ethics 20/20 in 2009,[36] and in the intervening years it has updated ethics rules to keep pace with the risks posed by cloud computing. In relevant part, the Commission added Rule 1.6(c) in recognition of the increased vulnerability of electronically stored information, including information in the cloud.[37]

Model Rule 1.6, Confidentiality of Client Information, articulates both a positive and a negative duty with respect to a lawyer's treatment of client information.[38] Rule 1.6(a) creates the negative duty whereby a lawyer may not reveal or disclose information relating to the representation of a client, and 1.6(c) creates the positive duty to proactively protect client information by "mak[ing] reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."[39] To adhere to this rule, lawyers must understand what

---

[36] *Commission on Ethics 20/20*, ABA, https://www.americanbar.org/groups/professional_responsibility/committees_commissions/standingcommitteeonprofessionalism2/resources/ethics2020hompeage/.

[37] ABA COMM'N ON ETHICS 20/20, REPORT TO HOUSE OF DELEGATES 4–5 (2012), *available at* https://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120808_revised_resolution_105a_as_amended.pdf.

[38] MODEL RULES OF PRO. CONDUCT r. 1.6 (AM. BAR ASS'N 2020) [hereinafter MRPC].

[39] MRPC r. 1.6(a), (c). Note also that the confidentiality obligation not to disclose applies to prospective clients through Rule 1.18(b), and to past clients through Rule 1.9(c)(2). Rules 1.18(b) and 1.9(c)(2) were not revised to apply the positive duty to protect against inadvertent or

it is to "reveal" or "disclose," what comprises "unauthorized disclosure" and "unauthorized access," and what counts as "reasonable efforts."

One could infer that "unauthorized" refers to authorization by the client, rather than authorization by the lawyer or the company providing the cloud-connected voice-computing device. This inference is based on Rule 1.6(a), which uses the term "authorized" to refer to implied authorization by the client as one situation in which lawyer disclosure is permitted.[40] Nonetheless, in this context, where there is more than one potential meaning of "authorization," it would be helpful if the ABA made the meaning of "unauthorized access" and "unauthorized disclosure" explicit. Further, the grammatical structure of Rule 1.6(c) makes explicit that the "inadvertent" descriptor applies only to disclosure—in other words, the rule does not recognize or address the prevention of inadvertent access. [41] The difficulty of finding a dividing line between disclosure and access in the technology context is a persistent one.

The comments to Rule 1.6 also provide some guidance on the meaning of "reasonable efforts."[42] Reasonableness is based upon factors including the sensitivity of the information, the risk of disclosure without further safeguards, the difficulty of employing further safeguards, and the cost of employing further safeguards.[43] The reasonableness inquiry thus involves

---

unauthorized disclosure as provided in Rule 1.6(c), but it would seem reasonable to read in the positive duty. Comment 20 to Rule 1.6 points in that direction by stating that the "duty of confidentiality" (as opposed to, say, Rule 1.6(a) only) applies to past clients via Rule 1.9.

[40] MRPC r. 1.6(a) cmt. 5. Rule 1.6(a) also allows disclosure if the client gives (express) "informed consent," and Rule 1.6(b) lists several other exceptions to the duty of confidentiality.

[41] MRPC r. 1.6(c).

[42] "Reasonable" or "reasonably," when referring to conduct, is defined under Rule 1(h) as the "conduct of a reasonably prudent and competent lawyer." MRPC r. 1.0(h).

[43] MRPC r. 1.6 cmt. 18. *See also id.* cmt. 19 (adding that "[w]hen transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to

balancing several factors by way of a cost-benefit analysis. Neither Rule 1.6 nor its comments, however, offer much clarity on what counts as "disclosure," except for one comment stating that disclosures include not only the direct disclosure of client information, but also the revelation of information that "could reasonably lead to the discovery of such [protected] information by a third person."[44] "Access" is not defined or explained at all.

### B. The Restatement of the Law Governing Lawyers

The Restatement captures the same duties articulated in Rule 1.6 in its own § 60, recognizing a similar negative duty "not [to] use or disclose confidential client information . . . if there is a reasonable prospect that doing so will adversely affect a material interest of the client," and a positive duty to "take steps reasonable in the circumstances to protect confidential client information against impermissible use or disclosure by the lawyer's associates or agents that may adversely affect a material interest of the client . . . ."[45] The Restatement recognizes a third duty, protecting against the lawyer's use of confidential information for self-enrichment, but that is unrelated to our inquiry.[46] In commentary to § 60, A Lawyer's Duty to Safeguard Confidential Client Information, the Restatement defines disclosure of information as "revealing the information to a person not authorized to receive it and in a form that identifies the client or client matter either expressly

---

prevent the information from coming into the hands of unintended recipients").

[44] MRPC r. 1.6 cmt. 4.

[45] RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS § 60 (Am. Law Inst. 2000) (hereinafter RESTATEMENT). Interestingly, a literal reading of the positive duty articulated in §60(b) includes no directive that the lawyer "take steps" to prevent her own impermissible disclosure. This is likely an omission; the correct reading takes into consideration the clarification in comment d that §60 is intended to include the lawyer's own precautions to safeguard client confidential information. Nonetheless, on this issue, Model Rule 1.6(c) is clearer.

[46] *Id.* The Model Rules' prohibition against using (as opposed to revealing) confidential information is found in Rule 1.8(b) for current clients, 1.18(b) for prospective clients, and 1.9(c)(1) for past clients.

or through reasonably ascertainable inference."[47] Based on this definition, there is no "disclosure" if the revealed information cannot be linked to the client; in other words, a certain quantum of identifying information must be satisfied for a revelation of information to be a "disclosure."

The Restatement also recognizes instances when there is a clear disclosure, but it is a permissible one. The permissibility of a disclosure is generally tied to the purpose of the disclosure and the identity of the recipient. For example, the Restatement allows "[d]ivulgence to facilitate practice of law," meaning that disclosures to facilitate the lawyer's practice and which are not expected to cause harm to the client are acceptable.[48] These disclosures may be made to employees within the lawyer's firm (office managers, clerks, administrative assistants) or to confidential independent consultants (IT professionals, accountants, etc.).[49] On this point, the Restatement and Model Rules do not differ significantly; Rule 1.6(a) allows disclosure that "is impliedly authorized in order to carry out the representation," and Comment 5 to the Rule clarifies that implied authority includes disclosure within a law firm.[50]

While the Restatement, unlike the Model Rules, offers a definition of disclosure, the Restatement's definition does not aid us in interpreting what the current version of Model Rule 1.6 requires. First, the Restatement was promulgated in 2000, and has not been revised in light of the MRPC's 2012 updates. In particular, the 2012 updates added Rule 1.6(c) and comments 18 and 19, which, unlike the Restatement, require reasonable efforts to protect against *unauthorized access* as well as *inadvertent* or *unauthorized* disclosure.[51]

Second, taking into account the common meanings of "access" and "disclosure," the risk of unauthorized access is a

---

[47] RESTATEMENT § 60 cmt. c(i).
[48] RESTATEMENT § 60 cmt. g.
[49] *Id.*
[50] MRPC r. 1.6(a) & cmt. 5.
[51] MRPC r. 1.6 & cmt. 18 (emphasis added).

far more frequently occurring possibility than unauthorized disclosure of client confidential information. [52] In this context, access is the mere possibility or ability to obtain the information, whereas disclosure goes further—the information has been exposed or made known. One might say that any unauthorized disclosure involves unauthorized access as well, although not all access inevitably leads to disclosure, because a third person may have access that is never exercised. Under the Restatement, however, even access that is exercised may fail to comprise a disclosure. Client information may be recorded and stored in manners that do not identify the client or the client matter or allow the client's identity to be determined by reasonable inference, and so would not be a disclosure under the Restatement's definition, and yet the information may be accessible by unauthorized third persons. The narrow definition of disclosure under the Restatement, which does not address issues of access, forces us to examine the meaning of "disclosure" as compared with "access" under Rule 1.6.

The Model Rules clearly warn against inadvertent or unauthorized disclosure *and* unauthorized access (but not inadvertent access),[53] so practitioners may infer that the writers meant something different by "access," rather than "disclosure."[54] But it is unclear whether Rule 1.6 "access" requires that the client's identity be ascertainable from the accessible information (making MRPC "access" the same as Restatement "disclosure"), or if Rule 1.6 access requires no particular quantum of identifying information (meaning MRPC

---

[52] *Access*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/access ("freedom or ability to obtain or make use of something . . ."); *Disclose*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/disclose ("to make known or public . . . to expose to view").

[53] One may argue that "inadvertent access" must be the result of a lawyer's poor understanding of the technology they are using, and thus rises to the level of a failure to maintain competence per Rule 1.1 comment 8. Even so, teasing out the difference between an inadvertent disclosure (covered by Rule 1.6) and inadvertent access (not covered by Rule 1.6) as depending upon some factual particularity to the function of the technology that was used seems arbitrary.

[54] MRPC r. 1.6(c).

"access" may be a lower bar to satisfy than Restatement "disclosure"). Did the drafters of the Model Rules intend a broader definition of "disclosure" than the Restatement, or did the Model Rules' addition of "unauthorized access" otherwise modify what comprises a disclosure, instead of access?

Third, the Restatement does not clarify whether "disclosure" is limited to intentional acts or whether the reference to "impermissible" disclosure includes "inadvertent" acts, as Rule 1.6(c) expressly does.[55] Fourth, the Restatement definition of "disclose" in terms of "reasonable ascertainment" of client identity does not give us enough detail to establish whether revealing the information to Google Home or Amazon Alexa counts. Some may argue that making client information known to a digital assistant is not making it known directly to a human,[56] and human review of the information may be unlikely; on the other hand, the device is designed to make recordings, and a portion of recordings are absolutely destined for human review. Finally, the Restatement definition of "disclosure" also does not clarify whether a single revelation of information that does not contain enough information to identify a client or matter may tip the scale into a disclosure when combined with other instances over time.[57] In short, the Restatement does not help resolve interpretive questions of Model Rule 1.6, and in particular 1.6(c).

### C. ABA Ethics Opinions

---

[55] Comment d to §60 of the Restatement does reference "inadvertent," but only in the context of waiver of attorney-client privilege. RESTATEMENT § 60 cmt. d.

[56] Again, seeing how "access" might fit into the Restatement would be helpful here, as the circumstances described could be cast as giving unauthorized (or inadvertent) access, rather than disclosure.

[57] For example, a single recorded snippet of a word may be meaningless standing alone, but recurring snippets of the word over a longer period of time could accumulate to result in a "reasonably ascertainable inference" of the identity of a target of a planned litigation or merger, or the identity of a client, which would be a "disclosure" under the Restatement definition. Of course, keep in mind that even if there is a disclosure, it is not necessarily a violation.

About twenty years ago, the ABA released Formal Opinion 99-413, walking through the confidentiality analyses underlying various technologies in use by lawyers at the time.[58] The analysis of land-line telephones balanced the lawyer's undisputed reasonable expectation of privacy[59] against the "substantial risk of interception and disclosure" inherent in using a phone.[60] Although the opinion described the ease with which telephone communications may be tapped, it concluded that, "[d]espite this lack of absolute security in the medium, using a telephone is considered to be consistent with the duty to take reasonable precautions to maintain confidentiality."[61]

With respect to all types of email discussed ("direct," "private system," online service provider, and internet email), the Committee found that despite some risk of interception, the reasonable expectation of privacy in e-mail communications rendered its use consistent with Rule 1.6.[62]

Cellular phone calls were thought to be a bit different from the deemed-safe land-line and e-mail communications.[63] This distinction might seem odd to modern readers, who are accustomed to cellular phones, which are not merely cordless phones, but rather small computers,[64] and which have

---

[58] Formal Op. 99-413, *supra* note 17 (discussing protecting the confidentiality of various methods of communication, such as unencrypted e-mail).

[59] The opinion appeared to use the term "reasonable expectation of privacy" in the same way courts employ it in Fourth Amendment search and seizure jurisprudence.

[60] Formal Op. 99-413, *supra* note 17.

[61] *Id.*

[62] *Id.*

[63] *Id.*

[64] We tend to think of cell phones as smartphones, but Formal Op. 99-413 was written when "dumb phones," which only made calls and sent text messages with limited or no internet capability, were still very common. PDAs and early smartphones were available in the early 2000s, but it was not until the release of the first iPhone in 2007 that smartphones began to resemble the devices we are familiar with today. *See Press Release: Apple Reinvents the Phone with iPhone*, APPLE (Jan. 9, 2007), https://www.apple.com/newsroom/2007/01/09Apple-Reinvents-the-Phone-with-iPhone/.

increasingly replaced landlines.[65] The committee found that cell phone calls were subject to the risks associated with land-line phones as well as interception via public radio waves.[66] Of key importance to the ABA was the fact that "the intercepted signals of cordless and analog cellular telephones are in an instantly comprehensible form (oral speech), unlike the digital format of e-mail communications."[67] The committee did not express an opinion about cellular phones, but noted that there was divided authority on the subject in 1999, and that cell phones embodied concerns not raised by either e-mail or land-line phones alone.[68] The application of this opinion to the instant examination of voice computing plus cloud computing is clear: the instantly comprehensible form of captured data presents a concern that was not implicated by predecessor technologies.

In 2011, the ABA released an opinion elaborating upon the reasonable expectation of privacy in e-mail in the hypothetical situation of a client using work email to communicate with their attorney while the client was engaged in an employment dispute.[69] In this situation, the ABA found that the employer's significant incentive to access the client-employee's email, which the employer's internal policy presumably allowed, resulted in a climate of heightened risk that required the lawyer to warn their client against using a business computer or email for substantive communications with counsel.[70] Here too there is room to draw a connection to voice computing and cloud computing. Large companies with successful voice-controlled cloud-computing devices have a

---

[65] *See* Philip Bump, *Most Adults Live in Wireless-Only Households – and Where That Varies Is Important*, WASH. POST (Jan. 7, 2018), https://www.washingtonpost.com/news/politics/wp/2018/01/07/most-adults-live-in-wireless-only-households-and-where-that-varies-is-important/.

[66] Formal Op. 99-413, *supra* note 17.

[67] *Id.*

[68] *Id.*

[69] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 11-459 (2011).

[70] *Id.*

high incentive to invest in human review of captured audio in order to improve their technologies and compete with one another;[71] like employers who have in place policies allowing review of employee activity on work computers, companies who produce voice-controlled, cloud-computing technologies may certainly include within their privacy policies allowances for reviewing recordings to improve service. Of course, there is a difference in that employers may justify examining the contents of monitored employee emails to ensure that the employees are working and not wasting resources. Tech companies who only collect data to improve voice-computing software do not have a similar justification for monitoring the content of consumer communications, unless, as some sources suggest, they are deliberately trying to gather personal information from the communications as well.[72]

A more recent opinion from 2017, Opinion 17-477, retained the reasonable expectation of privacy analysis, but moved the needle on email to find that some forms of unencrypted email may be insufficiently secure for the transmission of sensitive client communication because of the rising prevalence of "cyber-threats" and the vulnerability of unsecured networks.[73] The ABA explained that, since the issuance of Opinion 99-413 in 1999, the variety of methods and devices used to create and store client confidential communications has multiplied, with "each device and each storage location offer[ing] an opportunity for the inadvertent or unauthorized disclosure of information relating to the representation, and thus implicat[ing] a lawyer's ethical duties."[74]

---

[71] Estes, *supra* note 3 (noting that "companies like these with data-driven business models have every incentive to collect as much information about their users as possible.").

[72] *Id.*

[73] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 17-477 (2017) [hereinafter Formal Op. 17-477] (discussing requirements for securing the communication of protected client information).

[74] *Id.*

### 1. How the Duty of Competence Informs the Confidentiality Analysis

Formal Opinion 17-477 advocates for a case-by-case, fact-based analysis to gauge the level of care that must be taken in consideration of the level of sensitivity of the client confidential information at issue.[75] This is the same analysis outlined in comment 18 to Rule 1.6(c).[76] The non-exhaustive list of factors includes the sensitivity of the information, the likelihood of disclosure without additional safeguards, the cost of using additional safeguards, the difficulty of implementing those safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent their client.[77]

In the context of technology, the duty of competence plays a key role in facilitating a lawyer's adherence to the Model Rules. Model Rule 1.1 mandates that a lawyer "shall provide competent representation to a client."[78] In 2012, the ABA elaborated that competent representation includes an understanding of technology, updating Comment 8 to Rule 1.1 thus:

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.[79]

Under Model Rule 1.1 and Formal Opinion 17-477, attorneys must understand how client information is transmitted and where it is stored in order to make an educated decision about the appropriate method of communication to employ. A method of communication that is reasonable for one purpose (such as confirming the date of an appointment) may

---

[75] *Id. See also* Black, *supra* note 12.
[76] *See supra* notes 42, 43.
[77] Formal Op. 17-477, *supra* note 74.
[78] MRPC r. 1.1.
[79] MRPC r. 1.1 cmt. 8 (emphasis added).

be inappropriate for another purpose (such as discussing the information gathered in a deposition).

The ABA reaches beyond the usual scope of its ethics opinions to lay out some specific steps that lawyers should take. The steps elaborated upon in Opinion 17-477 are as follows:

> 1. Understand the nature of the threat.
>
> 2. Understand how client confidential information is transmitted and where it is stored.
>
> 3. Understand and use reasonable electronic security measures.
>
> 4. Determine how electronic communications about clients' matters should be protected.
>
> 5. Label client confidential information.
>
> 6. Train lawyers and nonlawyer assistants in technology and information security.
>
> 7. Conduct due diligence on vendors providing communication technology.[80]

While the information in this opinion provides far more granular and detailed guidance than normally offered by ABA ethics opinions, the challenge of applying this methodology is that many commonly occurring scenarios involve the use of a personal device. These guidelines on vetting technology and educating people presume intentional use of a technology that has been deliberately adopted by a legal practice.[81] A competent lawyer must nonetheless understand that inadvertent

---

[80] Formal Op. 17-477, *supra* note 74.

[81] Note also that with intentional adoption, Rules 5.1 and 5.3 impose upon some lawyers the supervisory responsibility of ensuring others comply with appropriate measures as well. MRPC r. 5.1, 5.3. When considering outsourced support services, lawyers should also consult ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 08-451 (2008).

use of personal technology poses a similar risk to client confidential information as speaking within earshot of a stranger. Lawyers should not be able to claim in cases of deliberate use that they did not know of these risks, and therefore acted "unintentionally." Put another way, "reasonable efforts" under Rule 1.6(c) should be read to incorporate the duty to act competently in keeping abreast of the risks and benefits of technology under Rule 1.1 Comment 8.[82]

## III. PART THREE

Part II supplied a summary of the existing guidance on confidentiality and the gaps in that guidance. Part III now extends the analysis. Section A of Part III suggests reasonable measures that a lawyer may take to satisfy her duty of confidentiality, describing and analyzing various risk-mitigating strategies relevant to the technology at issue. Section B then anticipates a series of four hypothetical scenarios and walks through how to assess the risks presented and choose appropriate reasonable measures to employ.

### A. Example Reasonable Measures

#### 1. Abstinence/Non-Adoption

One obvious safeguard against threats to confidentiality is for a lawyer to simply avoid the use of voice-computing, cloud-connected devices. For lawyers who have not yet adopted the devices in their home lives, this option is the path of least resistance for now. However, becoming a Luddite is no cure-all for issues of confidentiality. Even non-adopters are likely to have business with others who have adopted such devices; therefore, it is more appropriate for lawyers to learn substantively about how to identify risks and apply other risk-

[82] Even lawyers who make reasonable efforts under Rule 1.6, stay abreast of changes in technology under Rule 1.1, and properly supervise other lawyers or vendors under Rules 5.1 and 5.3 may experience a data breach. In the event of such a breach, other duties are triggered (like notifying clients under Rule 1.4). ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 18-483 (2018).

mitigating strategies than to rely upon avoidance of the technology.[83]

### 2. Siloing

Another safeguard is taking pains to silo work from home such that client information is never divulged in the presence of a voice-computing, cloud-connected device. Siloing as defined here relies upon the device essentially not being present when client information is present, so safeguards like muting the microphone do not fall under siloing—that precaution falls under the category of built-in settings. Any software or other technological safety measure which could possibly malfunction, be misused, or overridden is not siloing under this definition.

This safeguard is more easily described than executed. The practicability of siloing is challenged by any instance that requires working or taking a call from home—the current state of affairs under COVID-19 is a prime example, but many lawyers viewed themselves as on-call even before the current crisis. Of course, in combination with some actions explained below in Part III A.5, *Additional Protections*, a lawyer could effectively silo by deactivating or turning off their device whenever they plan to work in its vicinity.

### 3. Client Consent

This solution is one which hinges upon redefining any disclosures or access facilitated by the presence of a voice-computing, cloud-connected device as authorized disclosures rather than unauthorized ones. By explaining the risks and benefits associated with the use of voice-computing, cloud-connected devices and obtaining clients' informed consent to use such devices in her practice, a lawyer is not in violation of the Model Rules, even if client confidential information

---

[83] Kourtney Bitterly, *1 in 4 Americans Own a Smart Speaker. What Does That Mean for News?*, N.Y. TIMES OPEN (Aug. 22, 2019), https://open.nytimes.com/how-might-the-new-york-times-sound-on-smart-speakers-3b59a6a78ae3.

becomes unintentionally disclosed.[84] This safeguard succeeds only if the lawyer is well informed about the technologies she discusses with her client such that the lawyer's explanation is complete and accurate. As with all of the discussed safeguards, an essential underpinning of this safeguard is the competence of the lawyer.

#### 4. Built-in Settings

For those who plan to use voice-computing, cloud-connected devices, it is imperative to stay up-to-date with any and all profile settings, privacy settings, or data management options afforded to users. One tool in the lawyer's arsenal is to access and delete the audio that her device has recorded.[85] However, users must be aware that deleting the audio from their own device does not necessarily remove it from wherever it was sent for cloud processing. Additionally, while a lawyer can delete their own existing recordings and opt out of allowing Amazon, for example, to use their device's recordings to develop new features and improve machine transcription, they cannot opt out of allowing Amazon to retain their recordings for other purposes.[86]

Another simple measure is altering the sensitivity or responsiveness of the device,[87] or muting the device's

---

[84] Although a client can consent to disclosures incidental to the use of these devices, which protects against a 1.6(a) violation by the lawyer, it is not clear whether a client can consent to what would otherwise be a violation of Rule 1.6(c). It's possible that consent would make disclosure or access "authorized," but it's not so clear that a lawyer can contract out of the requirement to use reasonable efforts to prevent inadvertent disclosure.

[85] *See* David Nield, *How to Find and Delete Everything You've Ever Said to Your Digital Assistants*, GIZMODO (Nov. 6, 2019), https://gizmodo.com/how-to-find-and-delete-everything-youve-ever-said-to-yo-1839537890.

[86] An investigative journalist found that, despite opting out of recording retention in every instance permitted, Amazon still retained his Alexa recordings. *See* Estes, *supra* note 3.

[87] Henry St. Leger, *Stop Your Smart Speaker Eavesdropping with This Google Home Sensitivity Slider*, TECHRADAR (Apr. 22, 2020), https://www.techradar.com/news/your-google-home-smart-speaker-can-now-turn-down-the-volume-on-your-voice.

microphone to prevent recording.[88] This functionality is not found on all devices, so lawyers must take care to investigate a device's built-in capabilities before use. To investigate a device's network traffic (transmissions being sent by devices on one's network), lawyers can use a tool like the Princeton IOT Inspector.[89] Overall, the sufficiency of relying upon built-in features to make a voice-computing, cloud-connected device acceptable for use by lawyers must be determined on a case-by-case basis, depending on the individual device's capabilities and the work of the lawyer.

### 5. Additional Protections

The foremost protection a lawyer can employ is to be informed, not only of the capabilities of various devices, but of the presence of a device. A lawyer cannot tailor reasonable efforts to given circumstances without being aware of the presence of a device. For that reason, it is imperative for a lawyer to ask whether a device is present when conducting business in an unfamiliar setting.

To manage the presence of a device beyond muting it or turning it off, lawyers may benefit from the use of an add-on device to externally manage the voice-computing, cloud-connected device, and capture greater control for the device's user. There are both do-it-yourself and commercially available add-on devices designed to sit atop a smart speaker and overwhelm its microphone and always-listening functionality. Instead, the non-cloud-connected add-on device must be roused with a wake-word, and only then will the add-on device allow

---

[88] Because the function of devices is updated rapidly, this paper will not discuss instructions for implementing built-in privacy measures on individual devices, though the notion has been discussed by others. *See, e.g.*, Dave Taylor, *How Can I Mute My New Alexa (Amazon Echo) Smart Speaker?*, ASK DAVE TAYLOR (Dec. 31, 2019), https://www.askdavetaylor.com/how-to-mute-amazon-echo-alexa-smart-speaker/; Allen St. John & Thomas Germain, *How to Set Up a Smart Speaker for Privacy*, CONSUMER REPORTS (last updated Feb. 5, 2021), https://www.consumerreports.org/privacy/smart-speaker-privacy-settings/.

[89] PRINCETON IOT INSPECTOR (last visited Apr. 14, 2020), https://iot-inspector.princeton.edu/.

the smart speaker below to be awakened.[90] Recall that the main concern is the combination of voice computing and cloud computing; an add-on device that is always listening but not cloud-connected does not implicate the same concerns, because any audio captured is not going anywhere. These add-ons are a useful tool for smart speakers, but unfortunately, they do not address voice-computing cloud-connected devices that are not smart speakers. Although this paper focuses on smart speakers, devices like Apple watches, smartphones, and other appliances pose many of the same risks. The most effective form of protection may be one carried or worn by the lawyer, but such devices are not discreet and are not yet easily accessible by consumers.[91] When they do become more easily available, they may become must-have accoutrements for most lawyers.

### i. Questions Remain

Before diving into an application of the rules, readers should be aware that there are still more questions than answers. For example, Opinion 17-477 warns lawyers to understand how client confidential information is transmitted. Rule 1.6(c) adopts a negligence (reasonableness) standard with

---

[90] Bjørn Karmann & Tore Knudsen, *project_alias*, GITHUB (accessed Mar. 22, 2020), https://github.com/bjoernkarmann/project_alias; Paul Wagenseil, *This Gadget Promises to Stop Alexa and Google Home from Spying on You*, TOM'S GUIDE (Apr. 5, 2020), https://www.tomsguide.com/news/paranoid-smart-speaker-jammer; Dave Johnson, *Ensure your privacy around smart speakers with a $39 Paranoid auto-mute device*, CNET (Apr. 1, 2020), https://www.cnet.com/news/ensure-your-privacy-around-smart-speakers-with-a-39-paranoid-auto-mute-device/; Paranoid (last visited Apr. 6, 2020), https://paranoid.com/.

[91] Yuxin Chen, Huiying Li, Shan-Yuan Teng, Steven Nagels, Zhijing Li, Pedro Lopes, Ben Y. Zhao & Haitao Zheng, *Wearable Microphone Jamming* (2020), http://people.cs.uchicago.edu/~ravenben/publications/pdf/ultra-chi20.pdf; Kashmir Hill, *Activate This 'Bracelet of Silence,' and Alexa Can't Eavesdrop*, N.Y. TIMES (Feb. 14, 2020), https://www.nytimes.com/2020/02/14/technology/alexa-jamming-bracelet-privacy-armor.html.

respect to revealing information,[92] but it is not clear whether *transmission* per Rule 1.6 comment 19 and Opinion 17-477 requires any level of intent regarding the creation of a communication that reveals information (*e.g.*, the lawyer meant to transmit the information via voice call made on her Google Home), or if it merely requires the divulgence of information in a way that would be negligent depending on the level of knowledge required of a competent lawyer under Rule 1.1 (*e.g.*, the lawyer was reading aloud while vetting the terms of a deal at her dining table, and her Google Home picked up and transmitted some audio by false positive).[93]

There is no explicit guidance on whether the existence of client confidential information in the form of a sound recording comprises "unauthorized access" to that information by tech company employees who review recordings. And there are no data points on where the line is between disclosure and access, other than the common meanings of the words. Defining the threshold for disclosure or access bears further examination when one considers the odyssey that an utterance containing client confidential information could go through. When has a duty been breached?[94] Is it when an utterance is made in the presence of a device, when it is actually accessed and listened to by a human, or when it is further disseminated to other humans?[95] For now, the only option is to work with the

---

[92] *See* Formal Op. 18-483, *supra* note 83 ("[A]n attorney's competence in preserving a client's confidentiality is not a strict liability standard and does not require the lawyer to be invulnerable or impenetrable.").

[93] One commentator reports on particular words which increase the chance of a false positive. Digital Trends, *Words you shouldn't say around your smart speaker*, YOUTUBE (Apr. 7, 2020), https://www.youtube.com/watch?v=bCztxYMbo_k.

[94] The answer to this question may depend on whether the circumstances implicate Model Rule 1.6(a) or 1.6(c). A violation of 1.6(a) depends on what counts as a disclosure. A violation of 1.6(c) does not require a disclosure; it merely requires the failure to take reasonable efforts. Thus, it may not matter if a third party reviews the recordings for a 1.6(c) violation, so long as the lawyer failed to make reasonable efforts to prevent access or disclosure.

[95] *See* Day, Turner & Drozdiak, *supra* note 16 ("The [audio review] teams use internal chat rooms to share files when they need help parsing a

broad outlines of what the technology does and what ethical practice requires. Accordingly, the next section attempts to apply existing guidance to a series of common hypothetical scenarios.

## B. Hypothetical Scenarios

### 1. HYPOTHETICAL 1: When a Lawyer Knows of the Device and Uses It Intentionally

Suppose a lawyer asks her Google Home to set a reminder to make a call or add an item to the lawyer's to-do list. These commands could easily include client confidential information. It's true that the information may already have resided elsewhere under Google's management within the attorney's e-mail or calendar, but bringing client confidential information into the voice-computing realm reveals the information to people who would not otherwise gain access.

#### i. Application

To intentionally use a cloud-connected, voice-computing device to assist in their legal practice, a competent lawyer under Model Rule 1.1 must understand the benefits and risks associated with the technology.[96] The benefits are largely in efficiency and convenience, and have led to broad consumer adoption in home offices.[97]

---

muddled word—or come across an amusing recording."); *see also* Estes, *supra* note 3 ("[Amazon employees] can overhear compromising situations, and in some cases, the Amazon employees make fun of what people say.").

[96] MRPC r. 1.1 cmt. 8.

[97] *See supra* notes 31–34 and accompanying text. From 2018-19, the prevalence of smart speakers in home offices rose significantly. About 14.4% of smart speakers were estimated to be located in home offices by March 2019; the most popular locations for smart speakers in the home were the living room (44.4%), the bedroom (37.6%) and the kitchen (32.7%). [97] *Smart Speaker Consumer Adoption Report*, VOICEBOT.AI 12 (Mar. 7, 2019), https://voicebot.ai/wp-

The risks include many factors already discussed in Part I. Use of an always-listening device that is cloud-connected could expose a lawyer's speech to employees of the company producing the digital assistant, or to third parties to whom the data is sold.[98] As described in comment 18 to Model Rule 1.6 and in Formal Opinion 17-477, the sensitivity of the information to be transmitted should also factor into a lawyer's judgment.[99] When the information is not very sensitive (*e.g.*, audio snippets that would only reveal that the lawyer's firm is representing a company when it is already widely publicly known that they represent the company), the risk appears not to be significant enough to outweigh the usefulness of the technology. However, if the information is quite sensitive (*e.g.*, an audio snippet that would reveal the decision-making process behind a business negotiation[100]), then the risk taken by using the device is not a reasonable risk *if* the availability of the recording to behind-the-scenes digital-assistant company employees comprises "unauthorized access." Again, although it seems most likely that where there is access to information, it is probably unauthorized unless client consent is expressly given or can be implied, "unauthorized access" is still an untested linchpin of the current iteration of Model Rule 1.6.

---

content/uploads/2019/03/smart_speaker_consumer_adoption_report_2019.pdf.

[98] Anne Logsdon Smith, *Alexa, Who Owns My Pillow Talk? Contracting, Collateralizing, and Monetizing Consumer Privacy Through Voice-Captured Personal Data*, 27 CATH. U.J.L. & TECH. 187, 187 (2018) ("Personal data is easier than ever to obtain and virtually impossible to delete from the service provider once it's transmitted from the capturing device."); Stacy-Ann Elvy, *Paying for Privacy and the Personal Data Economy*, 117 COLUM. L. REV. 1369, 1373 (2017) (describing how companies monetize personal data).

[99] *See supra* note 75 and accompanying text.

[100] A journalist wrote of her Amazon Echo: "I was surprised when I checked my Amazon Echo recordings. In one recording, I was explaining why I wasn't taking a deal on a commercial building that I had for sale." Kim Komando, *How to Stop Your Devices from Listening to (and Saving) What You Say*, USA TODAY (Sept. 29, 2017), https://www.usatoday.com/story/tech/columnist/komando/2017/09/29/how-stop-your-devices-listening-and-saving-what-you-say/715129001/. The recording in that case was the result of a false positive trigger, but intentional use of the device clearly guarantees recording.

The bigger issue is "reasonable efforts"; the questions of whether lawyers must refrain from using voice-computing, cloud-connected devices, turn them off when discussing client matters, or seek express client consent for their use, all rest on the fact-intensive, case-by-case analysis promulgated in comment 18 to Model Rule 1.6 and Formal Opinion 17-477.

Use of a digital assistant by a lawyer in their daily life, such as for non-practice-related tasks around the house, is less of a threat to client confidentiality than to the lawyer's personal privacy, which is not the focus of this work.

### 2. HYPOTHETICAL 2: When a Lawyer Knows of the Device, but Does Not Intend to Use It

This hypothetical captures the archetypal case which causes the most concern among laypeople and privacy advocates—the "false positive" whereby a digital assistant records one's words although it was not intentionally addressed. The prevalence of this occurrence was commented upon during an explosion of journalism throughout 2019 on the "Big Five" tech companies (Apple, Google, Facebook, Amazon, and Microsoft) using human employees or contractors to analyze samples from voice assistant recordings.[101] The story was broken by Bloomberg with confidential sources from inside the companies, alarmingly noting that "in more than one out of 10 transcripts analysed by one of Bloomberg's sources, Alexa woke up accidentally."[102] Bloomberg reported that, "[s]ometimes listeners hear users discussing private details such as names or bank details; in such cases, they're supposed to tick a dialog box denoting

---

[101] Dorian Lynskey, *'Alexa, Are You Invading My Privacy?'— the Dark Side of Our Voice Assistants*, GUARDIAN (Oct. 9, 2019), https://www.theguardian.com/technology/2019/oct/09/alexa-are-you-invading-my-privacy-the-dark-side-of-our-voice-assistants ("[A]lthough the recordings are anonymised, they often contain enough information to identify or embarrass the user – particularly if what they overhear is confidential medical information or an inadvertent sex tape.").

[102] *Id.*

'critical data.' They then move on to the next audio file."[103] Although Bloomberg's source claims that 10% of reviewed clips were recorded in error, Amazon has tried to minimize the impact by countering that human staff review only fewer than one percent of conversations that are recorded.[104] Nonetheless, there is no indication that companies filter out or cease to review recordings that were made in error—on the contrary, those edge-cases that led to an erroneous recording are exactly what tech companies want to focus on in order to improve the accuracy of their devices. Research has indicated that the base number of false activations across devices remains high, at nearly one activation per hour of use.[105]

### i. Application

So, what is the upshot for lawyers? First, if a competent lawyer knows of the presence of the device in the room, the lawyer should not speak of sensitive matters *if* exposure of the information to a person reviewing audio files would comprise unauthorized disclosure or access to client confidential information. A competent lawyer is one who knows that speech in the presence of a voice-controlled, cloud-connected device has a small but distinct chance of being collected and reviewed and takes care accordingly.

Second, lawyers who do routinely use these devices, and reasonably expect that they may slip up and speak in the presence of a device, should meet this risk head on by anticipating it and informing their clients. This is more easily done at the initial engagement, where voice-controlled digital assistants may be discussed among any other technology used to facilitate the practice of law.[106] Lawyers who have

---

[103] Day, Turner & Drozdiak, *supra* note 16.

[104] Morrison, *supra* note 8.

[105] MON(IOT)R RESEARCH GROUP, *supra* note 7.

[106] For example, the Sedona Conference provides model clauses for an engagement letter in a publication on law firm data security. The Sedona Conference, *Commentary on Law Firm Data Security (Public Comment Version)* (Apr. 2020),

supervisory responsibility in law firms or other organizations where they work may have further obligations to ensure that these organizations include guidance on the use of certain technology among their internal policies.[107]

At the time of this writing, law firms are advising employees to work from home in the wake of the global COVID-19 pandemic. This surge of at-home work for attorneys has put a spotlight on the issue that voice assistants may result in companies like Amazon and Google hearing lawyers' confidential phone calls.[108] Such a state of affairs makes the need for wider lawyer competence vis-à-vis voice-computing, cloud-connected devices, and ethical guidance for the use of such devices, more urgent than ever.

### 3. HYPOTHETICAL 3: When a Lawyer Does Not Know of the Presence of the Device

---

https://thesedonaconference.org/publication/Commentary_on_Law_Firm_Data_Security.

[107] While the Model Rules apply only to individual lawyers and not to firms (with the exception of New York and New Jersey), Rule 5.1 does impose a supervisory responsibility upon certain individual lawyers within firms. Those attorneys shouldering supervisory responsibilities are the lawyers who should promulgate firm-wide policies (for example, on voice-computing, cloud-connected devices) as a way to "make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that all lawyers in the firm conform to the Rules of Professional Conduct." MRPC r. 5.1(a). Rule 5.3 on the supervision of non-lawyers is also relevant. MRPC r. 5.3.

[108] Crystal Tse & Jonathan Browning, *Locked-Down Lawyers Warned Alexa Is Hearing Confidential Calls*, BLOOMBERG LAW (Mar. 20, 2020), https://news.bloomberglaw.com/business-and-practice/locked-down-lawyers-warned-alexa-is-hearing-confidential-calls?context=search&index=0; Nelius, *supra* note 1 ("[Y]our Alexa or Google Home could be listening in on all those confidential work calls. Smart home devices not only listen to us when we don't want them too [sic], but we have no idea when an Amazon or Google employee is also listening to those conversations for the sake of 'improving voice-recognition features.'").

This scenario presents a thorny question which arises when a lawyer is in an unfamiliar setting[109]—either at another's office, another's home, or even in a hotel.[110] When participating in a meeting, must a lawyer ask their conversation partner or host, "Is there an Alexa/Google Home/etc. in this room?" Of course, the presence of an actual person is naturally commented upon before a meeting through introductions (*e.g.*, "This is John – he is a paralegal at the USAO."). Not so in the presence of a piece of technology ("This is Alexa, it helps me track billables.").[111]

### i. Application

In applying ABA guidance to Hypothetical 3, the identity of the lawyer's conversation partner gives rise to somewhat different issues and solutions. For example, if the conversation partner is another lawyer in the same firm, the solution could be a firm-wide policy that would cover both conversation participants on the use of devices. If the lawyer is speaking with her client, the lawyer could discuss the risks and benefits of voice-computing, cloud-connected devices with the client at the outset of the representation. If speaking with a lawyer from another firm (for example, as part of a joint defense team), the somewhat-awkward best course of action actually *is* to ask whether there is a device in the room. It will soon become the new normal to make such a query, and simply say that you're just trying to comply with the ethical obligations regarding confidentiality. Moreover, the mere presence of a voice-computing cloud-connected device will not preclude going on with the meeting. Instead, precautions can

---

[109] In fairness, the same concern is raised if the lawyer's conversation partner is remote and the conversation takes place over an audio or video call, but the audio is on speaker and audible to the whole room.

[110] Bryan Wroten, *Mute Smart Speaker Mics by Default*, HOTEL NEWS NOW (Feb. 28, 2020), https://www.costar.com/article/33124713 (discussing the problems produced by the emerging presence of smart speakers in hotel rooms).

[111] Randall Munroe, *Listening*, XKCD (last visited Feb. 28, 2021), https://xkcd.com/1807/ (illustrating a strategy for ascertaining the presence of an always-listening device).

be taken. For example, the device's microphone may be turned off manually when heightened security is required, or an additional device that increases the user's control over the digital assistant's microphone may be employed.[112]

### 4. HYPOTHETICAL 4: When a Lawyer Knows of the Device, but Another Person Does Not

This scenario is a mirror image of Hypothetical 3. In this instance, a lawyer owns the device or at least knows of its presence; thus, the lawyer is the participant with information while the lawyer's conversation partner would be unknowingly in the presence of a voice-computing, cloud-connected device.

#### i. Application

The foremost protection a lawyer can employ is to be informed, not only of the capabilities of various devices, but of the presence of a device. A lawyer cannot tailor reasonable efforts to given circumstances without being aware of the presence of a device. For that reason, it is imperative for a lawyer to ask whether a device is present when conducting business in an unfamiliar setting.

As in Hypothetical 3, the risks present and the appropriate actions to mitigate those risks depend upon the identity of the other person. When the unknowing person is the lawyer's own client, the clear course of action is to take one of the reasonable measures which disable the device, or to proceed in the presence of the device with the client's knowledge and authorization.

When the unknowing person is a lawyer from a different firm or some other party, instead of requesting information as in Hypothetical 3, it is the lawyer's duty to volunteer it. This exchange feels like a departure from the norm, but it is actually the new normal. When interviewed

---

[112] *See* Karmann & Knudsen, *supra* note 90 and accompanying text; *see also* Johnson, *supra* note 90 and accompanying text.

about the Google Nest Hub Max—the result of Google Home capabilities merged with the Nest— Senior VP of Google Devices and Services Rick Osterloh said, "[d]oes the owner of a home need to disclose to a guest? I would and do when someone enters into my home, and it's probably something that the products themselves should try to indicate."[113] This instinct in is line with the reasoning underpinning longstanding FCC regulation of telephone carriers, wherein devices were required to engage in some sort of notice and consent before recording.[114] On most smart speakers, including the Amazon Echo and Google Home, recording is indicated by the illumination of a small light, sometimes with the option of an activation sound.[115] It is not clear whether a small light or brief activation sound alone is sufficient—some would suggest that a verbal warning of activation is warranted, but that would also

---

[113] Leo Kelion, *Google Chief: I'd Disclose Smart Speakers Before Guests Enter My Home*, BBC NEWS (Oct. 15, 2019), https://www.bbc.com/news/technology-50048144.

[114] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 337 (1974) ("3. *FCC Regulations.* The FCC Regulations, in effect since 1948, require telephone carriers to file tariffs with the Commission to the effect that: 1.Adequate notice be given to all parties that their conversation is being recorded.").

[115] *Learn About the Lights on Your Speaker*, GOOGLE NEST HELP (last visited Apr. 10, 2020), https://support.google.com/googlenest/answer/7073219?hl=en ("Google Home, Google Nest Mini (2nd Gen), Google Home Mini (1st gen), and Google Home Max have LED lights on top that visually illustrate what they are doing."); *Nest Cam on Google Nest Hub Max*, GOOGLE NEST HELP (last visited Apr. 10, 2020), https://support.google.com/googlenest/answer/9449420?hl=en ("The LED light on your Nest Hub Max tells you what the Nest Cam is doing. When the Nest Cam is enabled, a solid green LED will be displayed on your device. This means that your Hub Max is ready to stream images or video to help you monitor your home remotely from the Nest app. When you or a family member is watching the live view, the LED will blink green."); *All Things Alexa: Alexa Help & Support*, AMAZON (last visited Apr. 10, 2020), https://www.amazon.com/b/ref=aeg_lp_hs_d_text/ref=s9_acss_bw_cg_aeglp_md1_w?node=17978646011&pf_rd_m=ATVPDKIKX0DER&pf_rd ("Your Echo device will communicate its status to you with visual indicators located on the device. You can also configure certain Amazon devices to play a short audible tone to signal the beginning and end of your request.").

make intentional use of the device more inconvenient (imagine beginning a verbal request of the device, only to have it interrupt your speech to inform you that it is listening.)

Lawyers should also be aware of the possible implication of Model Rule 8.4(a) if failing to inform a third person about the presence of a voice-computing, cloud-connected device could be construed as inducing another lawyer to violate the Rules of Professional Conduct with respect to that lawyer's own obligations.[116]

## IV. CONCLUSION

The conception of confidentiality put forth in Model Rule 1.6 is extremely broad by design. The rule is meant to be very protective of client information in order to promote the client's confidence in the security of any information that comes into her lawyer's possession as a result of representation, whether that information is provided directly by the client or not.

Now, the ubiquity of voice-computing, cloud-connected devices has created new hurdles for lawyers seeking to safeguard and avoid disclosure of client information. This paper has argued that lawyers need more explicit guidance to address these devices directly. Part I described the risks and benefits of the devices, and Part II highlighted key elements missing from current ABA guidance. In the interim, the best practice is for lawyers to calculate the risks presented by these devices on a case-by-case basis. As such, Part III offered suggestions to mitigate the risks and walked through a series of hypotheticals to assist practitioners in meeting their ethical duties. In sum, the benchmark for competence has moved, and with it, the conduct of a lawyer meeting her ethical duty of confidentiality. All must proceed armed with knowledge.

[116] *See* MRPC r. 8.4(a).