St. Mary's Law Journal

Volume 52 | Number 3 Article 6

10-29-2021

Alexa Hears with Her Little Ears—But Does She Have the Privilege?

Lauren Chlouber Howell

COMMENT

ALEXA HEARS WITH HER LITTLE EARS—BUT DOES SHE HAVE THE PRIVILEGE?

LAUREN CHLOUBER HOWELL*

* The author would like to thank her family and friends for all their encouragement throughout her life and law school career. In particular, she wants to express her deepest appreciation to her husband, David Howell; parents, Dean and Donna Chlouber; and brothers, Albert and Brian Chlouber and their families, for their unwavering support in her pursuit of her goals and dreams. The author would also like to thank the Volume 52 *Journal* Board and members, as well as her professional and scholastic mentors whose discussions and guidance helped to bring this Comment to fruition.

Finally, the author dedicates this Comment to her grandfather, Donald Wolf, who passed during law school but has continued to comfort, motivate, and inspire her. To the man who would always caveat any wisdom he shared by saying he was not well-educated, you should know you taught me so much more than most. "Love you always . . . you know that."

I. INTRODUCTION

Q: "Who done it? Where? And with what Weapon?"[1]

A: I suggest the crime was committed by the assistant, Alexa,[2] in the Study, with her Always-On Technology.[3]

In a scenario similar to the infamous game of Clue®, Alexa or the other assistants could either be the detective or the culprit—or both.[4] This principle is illustrated by Susan Allen in her comment entitled *Privacy in the Twenty-First Century Smart Home:*

> The existence and purpose of the Echo may seem innocuous enough as it serves as a personal in-home assistant meant to increase its user's convenience, yet it is vital to recall that unlike a human assistant that goes home at the end of every shift, the Echo is *always* listening.[5]

For those not yet well-acquainted with the assistants, Alexa and her friends—Siri, Cortana, Google, Bixby, and Moto (Voice)[6]—can be summoned from various devices such as cell phones or smart home speakers[7] and have valuable uses beyond playing music or giving the user

1. PARKER BROTHERS, CLUE INSTRUCTION BOOK 3 (2005), https://www.fgbradleys.com/rules/Clue.pdf [https://perma.cc/ATF3-2T39].

2. The Amazon Echo (Echo) or its respective assistant, Alexa, may be referred to individually throughout this Comment, but the statements and suggestions contained herein apply to virtual, personal, or digital assistants as a whole. *See generally* Maurice E. Stucke & Ariel Ezrachi, *How Digital Assistants Can Harm Our Economy, Privacy, and Democracy*, 32 BERKELEY TECH. L.J. 1239 (2017) (discussing the implications of the various digital assistants). They may also be referred to collectively as "assistants" or denoted colloquially with gendered pronouns.

3. *Cf.* PARKER BROTHERS, *supra* note 1, at 5 (instructing how to suggest the manner by which the crime was committed in gameplay, such as: "I suggest the crime was committed in the Lounge by Mr. Green with the Wrench.").

4. *See generally id.*

5. Susan Allen, Comment, *Privacy in the Twenty-First Century Smart Home*, 19 J. HIGH TECH. L. 162, 176 (2018) (emphasis added).

6. *See* Stacey Gray, *Always On: Privacy Implications of Microphone-Enabled Devices*, FUTURE OF PRIVACY F. 1, 6 (2016), https://fpf.org/wp-content/uploads/2016/04/FPF_Always_On_WP.pdf [https://perma.cc/VGC8-SHL3] (providing information regarding the speech activation of the various assistants and discussing the resulting implications); Bob O'Donnell, *Keeping Track of All These Voice Assistants Is Becoming a Problem*, FAST COMPANY (July 10, 2017), https://www.fastcompany.com/40437293/so-many-digital-assistants [https://perma.cc/8L46-UG7N] (introducing several of the assistants and how they operate).

7. *See* Robert D. Lang & Lenore E. Benessere, *Alexa, Siri, Bixby, Google's Assistant, and Cortana Testifying in Court*, 89 N.Y. ST. B.J. 8, 9 (2017) ("Although 'speech recognition' may sound like a lofty

today's weather.[8] For instance, they can make calls from the device itself once the user's phone is connected to the service,[9] quickly provide accurate answers to fairly complex mathematical questions,[10] keep track of attorneys' billable hours,[11] store patient or client information,[12] and more.[13] However convenient, the assistants have recently started making waves in

term, it simply refers to what most of us do daily, when we use our voices to ask our phones to dial our friends, our cars for directions, and our speakers to play our favorite songs. Speech recognition is 'the ability to speak naturally and contextually with a computer system in order to execute commands or dictate language.' Technology rivals are hard at work creating irresistible versions of easy-to-use devices with which we can talk and have questions answered.") (footnote omitted).

8. *See* Jason Beahm & Cameron Bowman, *Alexa, Are You a Snitch?*, 36 NO. 3 GPSOLO 56, 57 (2019) (describing the benefits of smart devices and the virtual assistants within them); Lang & Benessere, *supra* note 7, at 10 ("For most people, their virtual assistants' ability to always be listening for their 'wake words' is helpful. When we are driving, this allows us to complete tasks hands-free, avoiding distractions, as well as moving violations. While we are making breakfast in the morning, contemplating getting to work or to court on time, we can ask Alexa how long the morning commute will take. Alexa also allows us to use voice commands to turn on the light while walking into a dark room, without having to search for the light switch.")

9. *See* Jeffrey Allen, *Digital Virtual Assistants: Utility vs. Privacy*, 36 GPSOLO 4, 4 (2019) (describing a study of the fifteen most popular tasks performed by virtual assistants; although placing phone calls was absent from the list, the author notes he has noticed more people using their virtual assistant to place calls in the home, office, and car).

10. *See* Erika Rawes, *Amazon Alexa Is Great. But What If She Could Do More?*, DIGIT. TRENDS (Feb. 25, 2018, 5:00 PM), https://www.digitaltrends.com/home/what-if-alexa-could-do-more/ [https://perma.cc/P8NH-8SEU] ("Alexa does have tools that can solve problems like basic arithmetic equations, quadratic equations, and logarithms.").

11. *See* 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*, 61 RES GESTAE 41, 41 (2018) (noting virtual assistants can assist attorneys with recording their billable time); Whitney L. Hosey, Comment, *Alexa, Transmit Client Data to Amazon: Ethical Considerations for Attorneys Looking Forward to Virtual Assistants*, 19 WAKE FOREST J. BUS. & INTELL. PROP. L. 51, 56 (2018) (describing the process by which attorneys may track billable hours with Alexa). *But see id.* ("[T]here 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.").

12. *See* Steven Oberman, *The Ethical Use of Technology: Protecting You and Your Clients*, 43 CHAMPION 18, 18–19 (2019) (describing the necessity of protecting client information when it is stored digitally); Robert Humphreys, *How the Changes in Technology Are Shaping the Law and the Legal Profession in America*, 30 REGENT U. L. REV. 371, 389 (2017) (noting the relatively new ability to store client information in digital formats such as "the cloud," discussed *infra* Section II, and the risks associated with the same).

13. *See* Nelson & Simek, *supra* note 11, at 42 (describing other simple tasks virtual assistants are able to perform for the attorneys, thereby increasing efficiency in the workplace, including "adding entries to calendars, setting reminders, calling people in your contacts, [and] getting directions").

the legal community[14] due to the aforementioned privacy issues that arise from utilizing them for some of these seemingly innocent tasks.[15]

As admittedly vital as it is to keep these privacy issues in mind,[16] it is presumed many do not know the extent of Alexa's listening and recording capabilities.[17] If people are aware of the eavesdropping nature, it is likely they do not constantly consider it,[18] or they trust the receiver of the data to use it responsibly.[19] Prior to writing this Comment, the author rarely contemplated the ramifications of having multiple smart devices in her home and on her person at any given time. Similarly, others have expressed their lack of knowledge regarding the assistants' reach and how to overcome these unknowns.[20] For instance, Jeffrey Allen[21] commented:

14. *See* Lang & Benessere, *supra* note 7, at 10–12 (describing advantages and disadvantages of virtual assistants' use in the courtroom); Tom Mighell, *The Modern Personal Digital Assistant*, 42 L. PRAC. 30, 31 (2016) (admonishing not to "say anything to one of [the personal assistants] that you [do not] want discovered in the future").

15. *Digital Virtual Assistants*, *supra* note 9, at 4 (providing a list of the fifteen most common tasks requested of a virtual assistant).

16. *See* Allen, *supra* note 5, at 176 (encouraging keeping the privacy risks surrounding the virtual assistant in mind).

17. *See* Allison S. Bohm et al., *Privacy and Liberty in an Always-on, Always-Listening World*, 19 COLUM. SCI. & TECH. L. REV. 1, 5 (2017) (referencing a surprising 2015 privacy policy released by Samsung that "sparked the ire of [many] privacy advocates" when it stated: "Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data capture . . . and transmitted to a third party through your use of Voice Recognition."); Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 494 (2006) ("In many instances, people are not directly aware that they are being observed."); *Digital Virtual Assistants*, *supra* note 9, at 5 (drawing attention to a societal lack of awareness of the abilities of virtual assistants and available procedural safeguards).

18. *Cf.* Solove, *supra* note 17, at 495 ("In fact, there can be an even greater chilling effect when people are generally aware of the *possibility* of surveillance, but are never sure if they are being watched at any particular moment.").

19. *See* Bohm et al., *supra* note 17, at 5 ("You are vaguely aware that [the recorded voice data] . . . is stored on corporate servers, but you are not sure what information is stored, and you trust the company not to abuse it.").

20. Rani Molla, *People Say They Care About Privacy but They Continue to Buy Devices that Can Spy on Them*, VOX (May 13, 2019, 5:40 PM), https://www.vox.com/recode/2019/5/13/18547235/trust-smart-devices-privacy-security [https://perma.cc/XK3Y-6MMV] ("Even people who are tech savvy have a difficult time finding and understanding this information," according to an internet technology program manager. He also described a situation where a friend of his, well-versed in technology, "was 'tearing her hair out trying to find a baby monitor that was good for security and privacy.'").

21. Jeffrey Allen is the principal in an Oakland, California law firm, Graves & Allen. He is also Editor-in-Chief of *GPSolo* magazine, and he frequently speaks on technology topics. *Digital Virtual Assistants*, *supra* note 9, at 4.

> I cannot help but wonder what percentage of the customers even know that Amazon made the recordings, let alone that they have the ability to delete the recordings. I am fairly aware of things going on in the technological world. While I have known for some time that Amazon made the recordings and reviewed them, I did not know about deleting them until the release of the response [by Amazon] to [an inquiry by] Senator Coons [regarding Alexa's privacy practices].[22]

However, awareness regarding the reach of digital assistants is on the rise—and concerns are growing.[23] In a 2019 study by Microsoft, surveying 7,000 people, 72% reported using one of the aforementioned assistants via a smart device or through their vehicle.[24] Among those who reported using a digital assistant, "41% . . . reported concerns around trust, privacy and passive listening."[25] The other 59% should probably be concerned too.[26]

According to a Bloomberg article entitled *Amazon Workers Are Listening to What You Tell Alexa*, these concerns motivate millions not to allow smart home devices into their homes based on the fear the companies are listening.[27] Despite the rapid permeation of virtual assistants,[28] many users may not be aware of the plethora of legal, evidentiary, security, and privacy issues arising from (1) active and passive listening, (2) subsequent recording by the assistants, and (3) similar emerging technologies.[29]

---

22. *Id.* at 5.

23. *See* Katherine E. Tapp, Note, *Smart Devices Won't Be "Smart" Until Society Demands an Expectation of Privacy*, 56 U. LOUISVILLE L. REV. 83, 90–91 (2017) (discussing "the proliferation of personal smart devices" and the dilemma borne from "[t]he tension between technology and privacy"); Christi Olson & Kelli Kemery, *Voice Report from Answers to Action: Customer Adoption of Voice Technology and Digital Assistants,* MICROSOFT VOICE REP. 3, 23 (2019), https://advertiseonbing-blob.azureedge.net/blob/bingads/media/insight/whitepapers/2019/04%20apr/voice-report/bingads_2019_voicereport.pdf [https://perma.cc/H9SY-YTVF] ("Lack of trust is a significant factor hindering usage of smart speakers and digital assistants.").

24. *See* Olson & Kemery, *supra* note 23, at 8 (discussing the rising prevalence of digital assistants).

25. *See id.* at 6 (providing statistics regarding consumer distrust of digital assistants).

26. *See* discussion *infra* Sections II–IV.

27. *See* Matt Day et al., *Amazon Workers Are Listening to What You Tell Alexa*, BLOOMBERG (Apr. 10, 2019, 5:34 PM), https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio [https://perma.cc/QWC9-XYC4] (describing "[t]he Alexa voice review process").

28. Olson & Kemery, *supra* note 23, at 10 (declaring the majority of people have now "used voice search and voice commands through a digital assistant").

29. Devices such as drones, webcams, Nest Cam, Kapture, OrCam, and keystroke recording software may have similar ramifications. Gray, *supra* note 6, at 6.

This Comment explores some of these issues and offers two suggestions in an attempt to prevent the assistants from going too far and disclosing otherwise protected speech:

(1) Extend the protection of the existing privileges to the virtual assistants—allowing holders and claimants of existing privileges to block virtual assistants' disclosure of privileged conversations, so the assistants may not, in essence, testify against a person regarding speech which would normally be protected;[30] and

(2) Create a so-called "Castle" Privilege[31]—essentially protecting private utterances made in the presence of virtual assistants except in circumstances where a warrant was lawfully and reasonably obtained based on probable cause[32]—ensuring people feel comfortable in their own homes, where they would ordinarily have a legitimate expectation of privacy.[33]

II. BACKGROUND

Understandably, one of the issues which makes some people wary of virtual assistants is the privacy policies—or lack thereof—surrounding the waking procedure.[34] Each voice-activated assistant typically has an assigned wake word or phrase[35]—the utterance of which is intended to indicate the user would like the assistant to start listening and respond accordingly[36]—however, some of the assistants allow their owners to choose the word or phrase.[37] Although this can be a very convenient means of using the

30. *See* discussion *infra* Section IV.

31. *See* discussion *infra* Section IV.

32. U.S. CONST. amend. IV.

33. *See generally* Katz v. United States, 389 U.S. 347 (1967) (holding persons may have a reasonable expectation of privacy not only in their homes, but also in other areas—such as telephone booths—wherein there is a justifiable reliance on privacy).

34. *See* Raphael Davidian, *Alexa and Third Parties' Reasonable Expectation of Privacy*, 54 AM. CRIM. L. REV. ONLINE 58, 58 (2017) (discussing privacy implications connected to the waking of the assistants).

35. *See* Gray, *supra* note 6, at 6 (providing the assigned wake words of the speech activated assistants).

36. *See id.* at 5 (describing the ability of "speech activated devices . . . to remain in an inert state of passive processing, or 'listening,' for a pre-set 'wake phrase'").

37. *See id.* at 6 (discussing "wake phrases" of the various assistants).

assistant,[38] the technology surrounding waking the assistant is neither as simple, nor as full-proof as one might imagine—and has serious privacy implications.[39]

In order for the assistants to be summoned upon hearing the wake word or phrase, the devices must always be listening and are therefore sometimes referred to as "always-on" devices.[40] As noted by Amazon, Alexa begins recording a fraction of a second prior to the utterance of the wake word and begins transmitting it[41] to "the cloud."[42] Therefore, the Echo series of devices are always recording and just, hopefully, stop transmission to the cloud and delete the unintentional data compilation once the more advanced "cloud verification" denies detection of the wake word.[43]

Amazon has recently gone a step further, though, and filed a patent application which would allow Alexa to process commands prior to a wake word in order for users to interact more naturally with the device.[44] For example, the current command structure required to have an Echo device tell a joke is, "Alexa, tell me a joke," whereas under the new patent, one

38. *See* Beahm & Bowman, *supra* note 8, at 57 (balancing the convenience of the personal assistants and the associated privacy implications); Lenore Benessere & Robert D. Lang, *The Rise and Danger of Virtual Assistants in the Workplace*, BUS. L. TODAY (Feb. 15, 2018), https://businesslawtoday.org/2018/02/the-rise-and-danger-of-virtual-assistants-in-the-workplace/ [https://perma.cc/U7VG-88MT] [hereinafter *Rise and Danger of Virtual Assistants*] (discussing the convenient nature of voice-activated personal assistants); Allen, *supra* note 5, at 176 (emphasizing the fact that increased convenience is the intended purpose of digital assistants).

39. *See* discussion *infra* Sections II–III.

40. *See* Grace Manning, *Alexa: Can You Keep a Secret? The Third-Party Doctrine in the Age of the Smart Home*, 56 AM. CRIM. L. REV. ONLINE 25, 25 (2019) ("We rely on Alexa in our houses, and her always-on microphone to make life easier."); Steven I. Friedland, *Drinking from the Fire Hose: How Massive Self-Surveillance from the Internet of Things Is Changing the Face of Privacy*, 119 W. VA. L. REV. 891, 905–07 (2017) (discussing surveillance implications of the "Always-On Devices").

41. *See generally Alexa and Alexa Device FAQs*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=201602230&pop-up=1 [https://perma.cc/FC9Z-7CTB] (providing answers to frequently asked questions regarding the Alexa series of devices).

42. "Cloud storage is a cloud computing model that stores data on the Internet through a cloud computing provider who manages and operates data storage as a service." *Cloud Storage*, AMAZON, https://aws.amazon.com/what-is-cloud-storage/ [https://perma.cc/DJ7X-AS25].

43. *See Alexa and Alexa Device FAQs*, *supra* note 41 (discussing the Amazon cloud verification process); Gray, *supra* note 6, at 6 ("Until [the devices detect a key word], they remain in an inert state of buffering and re-recording, allowing the microphone to passively 'listen' for a key word without recording or transmitting information.").

44. *See* Pre-Wakeword Speech Processing, U.S. Patent No. 16/256376 (filed Jan. 24, 2019) (issued May 23, 2019) (publishing the patent application by Amazon for pre-wakeword speech processing).

could say, "tell me a joke, Alexa," and achieve the same results.[45] Based on the way the inventors describe the programming behind the audio retention and processing within this proposed system,[46] this plan would allow Amazon to retain significantly more recorded data.[47] Although this is a novel advancement, devices utilizing similarly constant and pervasive recording and retention technologies have historically evoked suspicion and criticism in the courts.[48]

Communications uttered around a smart device assistant are less secure if the assistant is set to wake via voice command, as mentioned above, as it can wake inadvertently.[49] For instance, communications around the Amazon Echo are not highly secure since the Echo is voice-activated and therefore records conversations in error when the assistant incorrectly perceives a wake word.[50] If a person says, "I was following a Lexus," a

45. *See id.* (describing Amazon's new "computer-implemented method for processing a spoken command when the wakeword does not begin the command").

46. *See id.* ("When the system detects a wakeword within a particular utterance, the system determines the most recent utterance change location prior to the wakeword and sends the audio from that location to the end of the command utterance to a server for further speech processing.").

47. Joseph Mandour, *Amazon Alexa Patent Will Record Even Before Wake Word*, MANDOUR & ASSOCS. (May 30, 2019), https://www.mandourlaw.com/blog/amazon-alexa-patent-will-record-even-before-wake-word/ [https://perma.cc/2DWX-KSXQ].

48. *See* Riley v. California, 573 U.S. 373, 395 (2014) (distinguishing the search of cell phones from physical records due to the inherent "element of pervasiveness"); People v. Majstoric, No. C082728, 2019 WL 5688702, at *1, 1 (Cal. Ct. App. Nov. 4, 2019) (holding a criminal defendant was not required to submit his technological devices for "search and seizure . . . any time of the day or night" after he accepted probation). In *Majstoric*, the court held such a condition was a violation of the defendant's constitutional rights, statutes, case law, and the privilege against self-incrimination. Supporting its conclusion, it quoted the Supreme Court of California, which had reasoned in another recent case:

> If we were to find this record sufficient to sustain the probation condition at issue, it is difficult to conceive of any case in which a comparable condition could not be imposed, especially given the constant and pervasive use of electronic devices and social media by juveniles today. In virtually every case, one could hypothesize that monitoring a probationer's electronic devices and social media might deter or prevent future criminal conduct.

In re Ricardo P., 446 P.3d 747, 754 (Cal. 2019).

49. *See* Peggy Wojkowski, *Alexa, Am I Violating Legal Ethics?*, KENT L. (May 31, 2017), http://blogs.kentlaw.iit.edu/islat/2017/05/31/alexa-violating-legal-ethics [https://perma.cc/F2U6-4R6H] (discussing the ramifications of virtual assistants that wake via voice command); Gordon K. Eng, *The Potential of New Digital Assistants for Office Use*, 40 L.A. L. 34, 35 (2017) (examining unintentional waking of the assistants).

50. *See* Eric Boughman et al., *"Alexa, Do You Have Rights?": Legal Issues Posed by Voice-Controlled Devices and the Data They Create*, BUS. L. TODAY, July 2017, at 2 (discussing accidental engagement of the assistant), https://www.americanbar.org/groups/business_law/publications/blt/2017/07/05_

nearby Echo device will likely wake due to misunderstanding "a Lexu--" as "Alexa."[51] If the individual were looking straight at the device and paying attention, they would see a blue circle light up on the device,[52] could command Alexa to stop,[53] or could even delve into their device's history to delete the inadvertent recording.[54] However, privacy concerns multiply if the person does not notice it has started recording as Alexa, by default, does not announce when she begins recording,[55] although users may enable the "start of request" sound.[56] Nevertheless, communications around devices that are set to wake by a method other than a wake word or phrase, such as pressing or holding a button, are considered more secure.[57] Although virtual assistants can similarly be unintentionally triggered via accidentally holding down the button,[58] this happens far less often than by inadvertent

boughman/ [https://perma.cc/EWD3-MJKX]; Manning, *supra* note 40, at 28 (describing a situation in which a murder occurred "and law enforcement hoped [Alexa] was accidentally triggered to record the events").

51. *See* Davidian, *supra* note 34, at 58 (providing an example of how the assistants may be woken inadvertently).

52. *See id.* at 59–60 (illustrating how Alexa notifies the user the interaction is being recorded). *But see* Craig Lloyd, *How to Make Your Amazon Echo Play a Sound When You Say "Alexa"*, HOW-TO GEEK (June 20, 2017, 4:53 PM), https://www.howtogeek.com/297966/how-to-make-your-amazon-echo-play-a-sound-when-you-say-alexa/ [https://perma.cc/PN8S-AC59] ("[I]f your Echo isn't someplace where you can see it easily, enabling the audio tones is a great way to make sure that Alexa heard you [or did not] without guessing.").

53. *See Commands | The Living List.*, THE ASSISTANT (2019), https://theassistant.io/commands/alexa/ [https://perma.cc/84UE-53EV] (providing an extensive list of commands to which Alexa responds).

54. In an Amazon FAQs section, *What about "false wakes"?*, Amazon acknowledges and addresses these inadvertent wake scenarios. They state a solution to this issue is to "review and delete the voice recordings associated with your account (including any audio resulting from a false wake) in your Voice History available in the Alexa app." *Alexa and Alexa Device FAQs*, *supra* note 41.

55. *See* David Flint, *Who's Listening to You?*, 38 BUS. L. REV. 70, 70 (2017) (illustrating privacy implications by virtual assistants generally).

56. *See Alexa and Alexa Device FAQs*, *supra* note 41 (describing how to enable "wake up" sounds either through the Alexa app or by voice request); Lloyd, *supra* note 52 (informing users this is not a universal feature and the setting will need to be adjusted for all Alexa devices).

57. For instance, iPhone users can choose to change their Siri settings to wake "her" by holding down the home button or holding down the power button, depending on the phone model, rather than by using the wake phrase. *See Digital Virtual Assistants*, *supra* note 9, at 6 (implying users may feel more comfortable enabling Siri to wake by pressing a button). Similarly, the newer Amazon Tap is more secure than its Echo counterparts as the user must touch the button to activate the microphone, meaning it is not listening constantly for the wake word or phrase, and the likelihood of inadvertently waking the device is less. *See* Wojkowski, *supra* note 49 (discussing features of the Amazon Tap).

58. *See* Candid Wueest, *Everything You Need to Know About the Security of Voice-Activated Smart Speakers*, SYMANTEC: THREAT INTEL. (Nov. 20, 2017), https://www.symantec.com/blogs/threat-intelligence/security-voice-activated-smart-speakers [https://perma.cc/UE3A-LRAX]; *see also*

voice activation. Additionally, the user has greater control over the data since the virtual assistant is not listening until the press of the button.[59]

If the smart device does not have an option to summon the assistant via pressing a button, the voice-activated device's security can be increased slightly by requiring the device to respond to certain voices, or at least limiting access to certain data depending on the user.[60] Some of the assistants respond to voices other than that of the purchaser, some respond to specified voice patterns and intonations, and some will respond to any voice by the default setting.[61]

III. CONCERNS

A. *Privacy Rights Under the Fourth Amendment*

> We live in a world of diminishing privacy. Walls and doors once protected our personal secrets from governments as well as nosy neighbors. Today, our hyper cyber-connected life has created ocean-sized data flows, a potent information marketplace, and public revelation of personal and even intimate secrets, some usually reserved in the past only for individual diaries or discussions behind closed doors. If a person lives "on the grid," her intimate and valued information sooner or later likely will be subject to access to third parties . . . . Significantly, big chunks of this information can end up in government hands, to be stored indefinitely and used without oversight.[62]

Gordon Eng, *Evaluating the Use of Digital Voice Recorders for the Law Office*, 26 L.A. L. 70, 70–71 (2003) (detailing similar issues that arose when users of digital voice recorders accidentally pressed buttons).

59. *See* Nelson & Simek, *supra* note 11, at 42 (explaining Samsung has opted to have Bixby respond by pressing a button).

60. *See id.* (pointing out although "Alexa can distinguish voices for access to some data, it is" still not as secure as it would be if it to require other access credentials); 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, 191–94 (2018) (discussing the possibility to create specific voice profiles, thereby increasing security over certain personal account data).

61. *See* Nelson & Simek, *supra* note 11, at 42 (describing some virtual assistants' abilities to differentiate between users' voices); *see* Smith, *supra* note 60, at 191 ("Google and Amazon have enabled their devices to distinguish between multiple users and associate their voice with their own personal account.").

62. Friedland, *supra* note 40, at 892. Anne Pfeifle, Comment, *Alexa, What Should We Do About Privacy? Protecting Privacy for Users of Voice-Activated Devices*, 93 WASH. L. REV. 421, 437 (2018) ("To keep pace with quickly changing technology, experts, scholars, and privacy advocates have proposed a number of solutions to protect users' privacy."); Allen Fiechuk, Comment, *The Use of AI Assistants in the Courtroom and Overcoming Privacy Concerns*, 28 WIDENER COMMONWEALTH L. REV. 135, 149–56

With emerging technologies on the rise in recent years, the right to privacy is the talk of the town like a new trend in this month's edition of Cosmo©, but its roots run deep and can be traced back hundreds of years.[63] In a famous English case, Sir Edward Coke stated: "[T]he house of every one is to him as his . . . castle and fortress, as well for his defence against injury and violence, as for his repose . . . ."[64]

Even more renowned on this side of the pond, the Fourth Amendment to the Constitution reads:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[65]

Although the entire Fourth Amendment is comprised of one fifty-four-word sentence,[66] courts are still trying to sift through the words in an attempt to discern how much protection the amendment provides, and to whom it provides, even those agreed upon protections.[67] The Framers did not provide us much guidance in analyzing these very important words.[68] As there are no explicit definitions or limitations helpfully appended to the text, constitutional interpretation is therefore left up to lawyers, lay-persons, judges, and justices alike.[69] Thousands of hours have been devoted to the

(2019) ("The court has recently begun to struggle with how AI fits in with a person's right to privacy, but as this technology is relatively new, the case law is almost non-existent.").

63. *See, e.g.*, U.S. CONST. amend. IV (prohibiting unreasonable searches and seizures).

64. Semayne's Case, 77 Eng. Rep. 194, 195 (K.B. 1604).

65. U.S. CONST. amend. IV.

66. *Id.*

67. *See* Jeffrey Bellin, *Fourth Amendment Textualism*, 118 MICH. L. REV. 233, 233 (2019) (attempting to find solutions for "the Fourth Amendment 'search' conundrums that continue to beguile the Court"); Trevor Burrus & James Knight, Katz *Nipped and* Katz *Cradled:* Carpenter *and the Evolving Fourth Amendment*, 2017 CATO SUP. CT. REV. 79, 79, 82 (2017–2018) (discussing "the Evolving Fourth Amendment" and the need "to help delineate when the Fourth Amendment has been triggered").

68. *See* Thomas K. Clancy, *The Framers' Intent: John Adams, His Era, and the Fourth Amendment*, 86 IND. L.J. 979, 979–80 (2011) (suggesting the route to a meaningful interpretation of the Fourth Amendment is through John Adams's "knowledge of, and views on, search and seizure and his role in formulating the principles to regulate those governmental actions" since he was the primary contributor to the Amendment).

69. *See* Bellin, *supra* note 67, at 233 ("Unfortunately, no viable alternatives appear on the horizon. The justices themselves offer little in the way of a replacement [to Fourth Amendment

meaning of these words, and thousands of pages of discussion and debate exist exploring the intricacies—and yet, it seems we are lifetimes away from figuring it out under the best-case scenario.[70]

B. *The Issue of Consent*

One thing is fairly clear, though—the right to privacy is not absolute.[71] Notwithstanding the above-listed issues,[72] which are discussed further in Section III,[73] consent can also be an affirmative defense to a claim of invasion of privacy.[74] Consent is "[a] voluntary yielding to what another proposes or desires; agreement, approval, or permission regarding some act or purpose, esp[ecially] given voluntarily by a competent person; legally effective assent."[75] Furthermore, consent may be express: clearly and unmistakably stated by the individual[76]—or it may be implied: inferred from the conduct of the individual.[77]

To further muddy the waters, the level of consent required for recordings depends on the jurisdiction in question: in some states, all parties need to consent to a recording, whereas federal law and a majority of states require consent of only one party.[78] In situations in which only one party's consent is required, some would purport that the owner or purchaser has consented

interpretation]. And scholars' proposals exhibit the same complexity, subjectivity, and illegitimacy that pervade the status quo.") (emphasis omitted).

70. *See* Clancy, *supra* note 68, at 983 ("Historical analysis remains a fundamentally important tool to interpret the words of the Fourth Amendment. Despite its crucial role, there is no consensus regarding the details or meaning of the historical record."). *See generally* Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 760 (1994) (criticizing the inconsistent interpretations of the Fourth Amendment).

71. *See* Kenneth Einar Himma, *Privacy Versus Security: Why Privacy Is Not an Absolute Value or Right*, 44 SAN DIEGO L. REV. 857, 864 (2007) (asserting privacy rights are not absolute—specifically mentioning the exceptions of security, "consent or some other legitimate authorization").

72. *See* discussion, *supra*, Section III(A) (mentioning, briefly, the issues of Fourth Amendment interpretation).

73. *See* discussion, *supra*, Section III(C) (delving into the varying interpretations of the prohibition of unreasonable searches and seizures under the Fourth Amendment).

74. *Consent*, BLACK'S LAW DICTIONARY (11th ed. 2019).

75. *Id.*

76. *Express Consent*, BLACK'S LAW DICTIONARY (11th ed. 2019).

77. *Implied Consent*, BLACK'S LAW DICTIONARY (11th ed. 2019).

78. *See* Jay Goldberg, *A Little Known Hidden Problem Within the Federal Wiretap Statute*, 14 NO. 9 WHITE-COLLAR CRIME REP. 1, 1 (2000) (discussing the Federal Wiretap Act and how consent requirements for recording conversations vary).

to the recording, but this is not a black and white matter.[79] When would consent occur, if it did at all? Would it be when a person buys the device, when they accept it as a gift, when turning it on, by leaving the assistant turned on or plugged in, when the assistant wakes, or if and when the person notices that it wakes? Since there is no express agreement between the user and the smart device and the duration of consent is not specified, the answer to this question is far from clear.[80]

Another issue rears its ugly head when visitors to a location speak, and Alexa records the speech, unbeknownst to them.[81] It has been suggested that third parties should enjoy a reasonable expectation of privacy in this situation[82]—and hopefully courts agree. If courts were to rule that the third parties have consented, there is a lot of grey area as to when that alleged consent may have occurred.[83] Considerations include, but are not limited to: awareness of the presence of the device,[84] awareness that the device is listening,[85] awareness that the device is recording and full understanding of the specific recording procedures,[86] awareness if the owner has their Alexa

79. *See* Supnick v. Amazon.com, Inc., No. C00-0221P, 2000 WL 1603820, at *2 (W.D. Wash. Dec. 6, 2002) ("Because Amazon did not disclose the scope of the electronic interception, plaintiffs assert that no one could have consented to the disclosure."). *See generally* Wilcosky v. Amazon.com, Inc., No. 2019CH07777, 2019 WL 2724009 (Ill. Cir. Ct. June 27, 2019) (alleging Amazon violated certain users' privacy rights by collecting biometric data without written releases from Alexa users).

80. *See* Smith, *supra* note 60, at 205–08 (addressing some of the contractual consent dilemmas surrounding virtual assistants).

81. *See id.* at 207 (differentiating visitors' consent from that of purchasers).

82. *See* Davidian, *supra* note 34, at 63 ("Considering the Court's willingness to find reasonable expectations of privacy with regard to activity taking place within homes, unless and until Alexa becomes customary and prevalent in homes, third parties without knowledge that Alexa was within their vicinity should have a reasonable expectation of privacy in their conversations under the Fourth Amendment.") (footnote omitted).

83. *See* Bohm et al., *supra* note 17, at 19–20, 29 (providing hypotheticals illustrating the uncertain nature of consent of third-party visitors); Davidian, *supra* note 34, at 61–62 (discussing consent issues with the assistants).

84. *See* Bohm et al., *supra* note 17, at 19–20, 29 (stressing visitors to a home or business containing a virtual assistant may not even be aware of its presence).

85. *See id.* at 16 (noting the smart "devices . . . are not marketed with sufficient information to enable consumers to understand and develop reasonable expectations about how the devices function—and when they are listening").

86. *See id.* at 16, 19–20, 29 (emphasizing visitors' potential lack of knowledge about virtual assistants' recording); Smith, *supra* note 60, at 207 (differentiating visitors' consent from purchasers' consent); Davidian, *supra* note 34, at 60 (hypothesizing there may be a day in the near future when all visitors to a home will understand they may be recorded by the assistants).

settings such that the recordings are sent to Amazon for quality control,[87] whether the speaker activated the device intentionally,[88] and whether the speaker was a minor or had reached the age of majority.[89]

A class action was recently brought under the California Invasion of Privacy Act "on behalf of a proposed class of 'all citizens of the State of California who used a household Amazon Alexa device while they were minors, but who have not downloaded and installed the Alexa app.'"[90] In most cases,[91] contractual agreements with minors are "voidable at the option of the minor" even if the minor has expressly agreed to the unspeakably long laundry lists of terms and conditions.[92] So why should they be bound to the chains of consent with recordings? They should *not*—but we will see how this shakes out in the coming years, especially with the recent innovation of the rainbow-ridden kids edition of the Echo Dot.[93]

C. *Unreasonable Searches and Seizures*

Among the ambiguous language in the Fourth Amendment is the phrase "unreasonable searches and seizures."[94] Although it may initially seem elementary, questions soon arise such as: what acts are deemed to be unreasonable, what is a search, and what is a seizure?[95] Black's Law

87. *See* Blake A. Klinkner, *Inviting the Spy into Your Office? Ethical Concerns Involving Attorney Use of Digital Assistants*, 41 WYO. L. 54, 54 (2018) (discussing complex questions surrounding digital assistants' use in the legal field).

88. *See* Boughman et al., *supra* note 50, at 2 (discussing the potential for accidental engagement of the assistant).

89. *See* Smith, *supra* note 60, at 218 (discussing potential violations of children's privacy laws by the virtual assistants).

90. R.A. v. Amazon.com, 406 F. Supp. 3d 827, 830 (C.D. Cal. 2019).

91. Exceptions exist, such as if "the minor . . . [fails to] disaffirm the entire contract within a reasonable time of reaching the age of majority." Juanda Lowder Daniel, *Virtually Mature: Examining the Policy of Minors' Incapacity to Contract Through the Cyberscope*, 43 GONZ. L. REV. 239, 244 (2007).

92. *See id.* at 244 ("Currently, most if not all jurisdictions allow a minor to disaffirm a contract made while he was under the age of majority solely based on his status as a minor.").

93. *See generally* Complaint, *In re* Request for Investigation of Amazon, Inc.'s Echo Dot Kids Edition for Violating the Child.'s Online Priv. Prot. Act (Fed. Trade Comm'n 2019), https://www.law.georgetown.edu/wp-content/uploads/2019/05/Echo-Dot-Complaint-FINAL-1.pdf [https://perma.cc/XT4K-8Y6H].

94. U.S. CONST. amend. IV.

95. *See* Julia R. Shackleton, *Alexa, Amazon Assistant or Government Informant?*, 27 U. MIAMI BUS. L. REV. 301, 310–11 (2019) (stating "[t]hroughout the course of Fourth Amendment jurisprudence, the United States Supreme Court has varied in its interpretation of what the Fourth Amendment protects"—providing examples from Justices Harlan's focus on the "subjective expectation of privacy" to Justices Taft's and Scalia's property or trespass-based notions of an unreasonable search).

Dictionary defines "unreasonable" as: "1. Not guided by reason; irrational or capricious. 2. Not supported by a valid exception to the warrant requirement."[96] A "search," as it pertains to criminal procedure, is "[a]n examination of a person's body, property, or other area that the person would reasonably be expected to consider as private, conducted by a law-enforcement officer for the purpose of finding evidence of a crime."[97] The definition[98] also echoes the Fourth Amendment's probable cause requirement[99] nested in the Warrants clause.[100] Lastly, a "seizure" is "[t]he act or an instance of taking possession of a person or property by legal right or process; esp[ecially], in constitutional law, a confiscation or arrest that may interfere with a person's reasonable expectation of privacy."[101]

Although the government has historically had a reputation for being the overreaching "Big Brother,"[102] sometimes it is valuable to have the right sort of big brother to look out for your interests.[103] On June 30, 1965, President Lyndon B. Johnson issued a memorandum addressing the wiretapping of telephones and the resulting invasions of privacy—urging these practices only be conducted in circumstances implicating a breach of national security.[104] What he went on to say was even more wise and insightful, far ahead of his time, and echoes principles that should be adhered to today regarding virtual assistants:

> Utilization of . . . electronic devices to overhear non-telephone conversations is an even more difficult problem, which raises substantial and unresolved questions of [c]onstitutional interpretation. I desire that each agency conducting such investigations . . . ascertain whether the agency's practices are

96. *Unreasonable*, BLACK'S LAW DICTIONARY (11th ed. 2019).

97. *Search*, BLACK'S LAW DICTIONARY (11th ed. 2019).

98. *Id.*

99. U.S. CONST. amend. IV.

100. *See Warrant Clause*, BLACK'S LAW DICTIONARY (11th ed. 2019) ("The clause of the Fourth Amendment to the U.S. Constitution requiring that warrants be issued only on probable cause.").

101. *Seizure*, BLACK'S LAW DICTIONARY (11th ed. 2019).

102. *See* Kenneth Shuster, *Stunting Big Brother's Growth: Reflections on* U.S. v. U.S. District Court, 18 HAMLINE L. REV. 64 (1994) ("[Reexamining] one of the most important Supreme Court cases to address governmental electronic eavesdropping . . . .").

103. *See, e.g.*, *Memorandum for the Heads of Executive Departments and Agencies* by President Lyndon B. Johnson (June 30, 1965) (quoted in United States v. Smith, 321 F. Supp. 424, 432 (C.D. Cal. 1971)).

104. *Id.*

> fully in accord with the law and with a decent regard for the rights of others.[105]

Two years later, in the landmark case of *Katz v. United States*,[106] the Supreme Court held the defendant, Katz, was protected from the warrantless eavesdropping by the government via a device placed outside the phone booth he was using as Katz had "justifiably relied" upon the privacy of the telephone booth.[107]

Shortly thereafter came Title III of the Omnibus Crime Control and Safe Streets Act of 1968, more commonly known as the Wiretap Act.[108] The Act prohibits unlawful seizure "of wire, oral, or electronic communications" by governmental and private agencies or individuals.[109] Although "[e]lectronic surveillance [has been said to be] an essential law enforcement tool,"[110] the digital assistants are recording and transmitting data unchecked, and therefore without probable cause.[111] It follows, then, that the limitations on how this collected data can be used must be at least as stringent, if not more so, than the constitutional, statutory, and common-law restrictions regarding wiretapping.[112]

Although Facebook has been complying with state and federal requests for Facebook users' data for years,[113] courts should find data from virtual assistants distinguishable. Even when a person directly and intentionally asks a virtual assistant a question, they do not have the same intent to publish that information as those who post on Facebook, Twitter, Instagram, and other forms of social media. In order "[f]or a conveyance

105. *Id.*

106. Katz v. United States, 389 U.S. 347 (1967).

107. *Id.* at 353.

108. 18 U.S.C. §§ 2511–23 (2018).

109. *Id.*

110. People v. Darling, 95 N.Y.2d 530, 535 (App. Div. 2000).

111. *See* Bohm et al., *supra* note 17, at 20–22 (arguing for the probable cause standard for access to always-on device information as this is not currently occurring).

112. *See* 47 U.S.C. § 605 (providing federal limitations on wiretapping); Benanti v. United States, 355 U.S. 96, 101 (1957) (holding neither participation nor knowledge by federal agents is required in order for the evidence obtained through wiretapping to be inadmissible in court); Lee v. Florida, 392 U.S. 378, 378, 381–82 (1968) (holding "continuous surreptitious surveillance and recording of all conversations" without consent "clearly amounted to interception of the petitioners' communications within the meaning of § 605 of the Federal Communications Act").

113. *See, e.g.*, Heidi M. Silton & Courtney Blanchard, *Social Media Discovery: The Ongoing Struggle to "Update Status"*, 69 BENCH & B. MINN. 16, 18 (2012) (providing information regarding Facebook's compliance policies with various types of subpoenas).

to be made voluntarily, it must be done with intent or by design, which, of course, presumes knowledge on the part of the consumer of that which is being conveyed."[114] This level of awareness is not yet commonplace with always-on devices.[115]

For this reason, the Florida Bar Association issued a Formal Ethics Opinion creating a process to ensure compliance with their local ethics rules regarding the use of smart devices and virtual assistants—the rationale behind the opinion being "that many lawyers were 'intentionally and unintentionally stor[ing] their clients' information on these [d]evices.'"[116] If highly-educated professionals struggle with unintentional recordings and data storage by the virtual assistants,[117] one can safely assume the dilemma does not stop there. Even more clearly deserving of protection, though, are the individuals inadvertently recorded due to an error in voice recognition by Alexa or her friends.[118]

Looking at recent case law regarding other digital intrusions can provide guidance in this matter. For instance, in a case wherein the police discovered a man, Kyllo, was growing marijuana indoors by aiming a thermal imager at his residence, the Supreme Court held that any information obtained from within the home that would ordinarily not have been accessible without physical intrusion, or without technology that is not in general public use, constituted a search.[119] The Court reemphasized "that the Fourth Amendment draws 'a firm line at the entrance to the house'" when it prohibits unreasonable searches and seizures.[120] In the 2014 case of *Riley v. California*,[121] two defendants were arrested and the digital contents of their cell phones were searched.[122] The Court deemed this was unconstitutional

114. Steven M. Bellovin et al., *It's Too Complicated: How the Internet Upends* Katz, Smith, *and Electronic Surveillance Law*, 30 HARV. J.L. & TECH. 1, 28 (2016) (footnote omitted).

115. *See* Bohm et al., *supra* note 17, at 5, 16, 19–20, 29 ("[I]t is often unclear to consumers what kinds of data these [always-on] devices are collecting, when they are collecting that data, and what companies are really doing with the data.").

116. Hosey, *supra* note 11, at 63 (quoting Fla. B. Ethics Op. 10-2 (2010)).

117. *See id.* (describing the ethical hoops attorneys are navigating in the virtual assistant arena).

118. *See* discussion *supra* Section II.

119. *See* Kyllo v. United States, 533 U.S. 27, 27 (2001) ("Where, as here, the Government uses a device that is not in general public use, to explore details of a private home that would previously have been unknowable without physical intrusion, the surveillance is a Fourth Amendment 'search,' and is presumptively unreasonable without a warrant.").

120. *Id.* at 40 (quoting Payton v. New York, 445 U.S. 573, 590 (1980)).

121. Riley v. California, 573 U.S. 373 (2014).

122. *See id.* at 378–81 (describing the arrests and subsequent searches and seizures of David Riley and Brima Wurie in each of their respective cases).

without a warrant.[123] The Court reasoned that due to the colossal storage capability of cell phones—often containing multiple years of sensitive data—an invasion of this variety is much more severe than physical searches of decades past.[124] As the Court stated, "many of the more than 90% of American adults who own cell phones keep on their person a digital record of nearly every aspect of their lives."[125]

Furthermore, in the 2011 case of *Carpenter v. United States*,[126] the Court arguably had excellent statutory reason to allow captured, warrantless evidence, but saw the following facts as crucial in finding otherwise.[127] After a series of robberies, several men were arrested in conjunction with the same, and one of the men detained eventually disclosed they had robbed many other locations and disclosed the names of his accomplices.[128] Upon obtaining this information, the court orders were sought—and granted—under the Stored Communications Act to obtain cell phone records for the accused.[129] The Stored Communications Act allows the government to compel certain communications records when there is reasonable cause to show the records are relevant and probative in an ongoing criminal investigation.[130]

The Court held the government obtaining the Defendant's cell-site location information (CSLI) violated his reasonable expectation of privacy, despite having obtained the data from a third party under a court order.[131] In doing so, it reasoned:

> Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's

123. *See id.* at 403 ("Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant.").

124. *See id.* at 375 (noting, prior to "cell phones, a search of a person was limited by physical realities and generally constituted only a narrow intrusion on privacy," but that in the modern world, a wealth of private information can be gathered from these devices).

125. *Id.*

126. Carpenter v. United States, 138 S. Ct. 2206 (2018).

127. *See id.* at 2211 ("This case presents the question whether the Government conducts a search under the Fourth Amendment when it accesses historical cell phone records that provide a comprehensive chronicle of the user's past movements.").

128. *Id.* at 2212.

129. *Id.*

130. *Id.*

131. *See id.* at 2219 ("In mechanically applying the third-party doctrine to this case, the Government fails to appreciate that there are no comparable limitations on the revealing nature of CSLI.").

> claim to Fourth Amendment protection. Whether the Government employs its own surveillance technology as in Jones or leverages the technology of a wireless carrier, we hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI. The location information obtained from Carpenter's wireless carriers was the product of a search.[132]

Although perhaps less obviously, the recording and repetition of speech by the virtual assistants is akin to the listening and repetition of speech by parrots.[133] In both situations, an eavesdropper of sorts repeats back information it overheard and was not expected to disclose. Courts have refused to admit such instances of testimony by parrots—despite parrots being regarded as highly reliable testimony from intelligent animals—for a number of reasons. In one case, a parrot named Max repeatedly cried out, "Richard, no, no, no!" after the murder of his owner, Jane Gill.[134] The defense attorney in the case wanted to have this evidence admitted because his client's name was Gary.[135] The attorney said it was not hearsay, but instead that it was akin to a recording device.[136] However, the Judge denied admission of the parrot's statement, despite expert testimony that this type of parrot has the ability to accurately repeat statements—especially in similarly stressful circumstances.[137]

Similarly, Bud, the parrot, began incessantly repeating, "Don't f***ing shoot!" after the murder of Martin Duram by Glenna Duram.[138] A parrot from South Carolina comparably repeated, "help me, help me," which had

132. *See Carpenter*, 138 S. Ct. at 2217 (stating, under exigent circumstances, CSLI data could foreseeably be lawfully obtained without a warrant).

133. *See* Christopher Coble, *Parrot Evidence Rule: Can Bird's Testimony be Admissible in Court?*, FINDLAW (July 21, 2017, 3:57 PM), https://blogs.findlaw.com/legally_weird/2017/07/parrot-evidence-rule-can-birds-testimony-be-admissible-in-court.html [https://perma.cc/KBE5-SVN7] (describing two instances in which words uttered by a parrot aided, or came close to aiding, in criminal cases); *Parrot May Have the Answer to a Killing*, N.Y. TIMES (Nov. 12, 1993), https://www.nytimes.com/1993/11/12/news/parrot-may-have-the-answer-to-a-killing.html [https://perma.cc/74H6-89RZ] (detailing how a California parrot named Max repeated information implying the death of his owner was unnatural); Tanya Roth, *Parrot's Comments Aid Cops in Elder Abuse Case*, FINDLAW (Dec. 14, 2010, 6:15 AM), https://blogs.findlaw.com/blotter/2010/12/parrots-comments-aid-cops-in-elder-abuse-case.html [https://perma.cc/J9AB-AKTZ] ("The case of a tattletale parrot may give police and prosecutors some real leads in a real story of alleged elder abuse in South Carolina.").

134. *Parrot May Have the Answer to a Killing*, *supra* note 133.

135. *Id.*

136. *Id.*

137. *Id.*

138. Coble, *supra* note 133.

been cried out by its owner, Anne Copeland, prior to her death. Even more heart-wrenchingly, the parrot also laughed, mimicking the laugh of Ms. Copeland's murderer.[139] There has been a push by the Nonhuman Rights Project for recognition of "certain 'cognitively complex' animals as 'persons' rather than 'things.'"[140] However, apparently their time has not come yet. Given this fact, that cognitively complex animals are still recognized as "things" and the recollections and resulting repetitions of "things" cannot be submitted as evidence in a case,[141] virtual assistants should not be any exception to that rule.

Traveling back in time, the court in *Dietemann v. Time*[142] hit the nail on the head when it held that the defendant infringed upon Dietemann's privacy rights by obtaining and publishing information about, and recordings of, the plaintiff without his consent.[143] The court eloquently reasoned:

> Plaintiff's den was a sphere from which he could reasonably expect to exclude eavesdropping newsmen. He invited two of defendant's employees to the den. One who invites another to his home or office takes a risk that the visitor may not be what he seems, and that the visitor may repeat all he hears and observes when he leaves. But he does not and should not be required to take the risk that what is heard and seen will be transmitted by photograph or recording, or in our modern world, in full living color and hi-fi to the public at large or to any segment of it that the visitor may select. A different rule could have a most pernicious effect upon the dignity of man and it would surely lead to guarded conversations and conduct where candor is most valued, *e.g.*, in the case of doctors and lawyers.[144]

D. *The Smart "Home Away from Home"*

Although many people tend to consider smart home devices as home accessories, hence their name, these devices also are finding their place in

139. Roth, *supra* note 133.

140. Tanya Basu, *Serious Question: Can a Parrot Act as a Witness in Court?*, THE CUT (Mar. 24, 2016), https://www.thecut.com/2016/03/serious-question-can-a-parrot-act-as-a-witness-in-court.html [https://perma.cc/YNN8-QFLV].

141. *Id.*

142. Dietemann v. Time, Inc., 449 F.2d 245 (9th Cir. 1971).

143. *See id.* at 248 (stating a person does not waive their privacy rights by inviting someone into their home).

144. *Id.* at 249.

the professional world—including in law firms and doctors' offices.[145] As the *Dietemann* court predicted,[146] this further illustrates the need for the above-mentioned privacy issues connected with virtual assistants to be adequately addressed.[147] Amazon has now developed *Alexa for Business*, which allows the user to keep track of billable hours, *inter alia*.[148] Additionally, Thompson Reuters has released its own Workplace Assistant.[149] However, with digital assistants on the rise, professionals will have to consider the Model Rules of Professional Conduct and applicable jurisdictional rules.[150]

E. *Evidentiary Considerations*

Some argue that digital assistants be used as so-called silent witnesses.[151] The silent witness theory is one in which a human witness is not required to substantiate an act occurred, but instead recordings specifically noted as photographs or videotapes are admitted as substantive evidence and do not require a sponsoring witness.[152] Taking no specific qualms with the silent witness doctrine generally, the digital assistants should not be included

145. *See* Beahm & Bowman, *supra* note 8, at 58 (discussing home and office use of the virtual assistants); *Rise and Danger of Virtual Assistants, supra* note 38, at 1 ("Virtual assistants processing and retaining your interactions in the Cloud raises privacy concerns and potentially creates a discoverable and admissible record with each use."); Robert D. Lang & Lenore E. Benessere, *Virtual Assistants in the Workplace: Real, Not Virtual Pitfalls and Privacy Concerns*, 21 J. INTERNET L. 1, 4 (2018) [hereinafter *Virtual Assistants in the Workplace*] ("Not surprisingly, as Alexa and other virtual assistants continue to increase in popularity, we are beginning to see them in both homes and businesses. If a virtual assistant is a luxury at home, then certainly, it is a necessity at work.").

146. *Dietemann*, 449 F.2d at 249.

147. *See* discussion *supra* Sections II–IV.

148. *See generally Alexa for Business*, AMAZON WEB SERVS., https://aws.amazon.com/alexaforbusiness/ [https://perma.cc/B7VH-A49A] (discussing various professional applications of the Alexa for Business product). *See Virtual Assistants in the Workplace*, *supra* note 139, at 3–4 (discussing the *Alexa for Business* platform); Wojkowski, *supra* note 49 (drawing attention to systems designed to bring Alexa into the legal workplace).

149. *See* Wojkowski, *supra* note 49 (providing another example of a legal system which can be utilized through Alexa).

150. *See* MODEL RULES OF PROF'L CONDUCT R. 1.1 (AM. BAR ASS'N 2018) (laying guidelines for attorney competence); *id.* R. 1.6 (establishing guidelines for confidentiality of information).

151. *Alexa, Did He Do It? Smart Device Could be Witness in Suspicious Florida Death*, GUARDIAN (Nov. 1, 2019, 4:21 PM), https://www.theguardian.com/us-news/2019/nov/01/alexa-florida-death-witness-amazon-echo?CMP=share_btn_link [https://perma.cc/2EYB-NXWU] [hereinafter *Alexa, Did He Do It?*].

152. *See generally* Tracy B. Farrell, *Construction and Application of Silent Witness Theory*, 116 A.L.R.5th 373 (2004) (discussing how most jurisdictions do not require significant foundation to successfully illicit silent witness testimony).

under this theory for several reasons: (1) their recordings and transcriptions are not photographs or videotapes; (2) the digital assistants are so pervasive in society at this point that they are practically unavoidable;[153] and (3) the activation or waking technology is far from perfect.[154] Photographs and videotapes are much more time-honored types of recorded evidence. Therefore, it follows they should be more reliable than digital assistants. Even if a court were to rule that they should be considered silent witnesses, the privilege extension to the digital assistants[155] should still apply to confidential communications, but only to the extent permitted under the applicable state and federal rules.

To illustrate, there is an investigation underway in Hallandale Beach, Florida, wherein police believe recordings captured by Alexa may help them get to the bottom of a woman's death.[156] Sylvia Galva Crespo and her husband were arguing and, somehow, she was stabbed in the chest.[157] Should the court find that Alexa's recordings of the altercation, if any, are admissible under a silent witness theory? The recordings would likely still be admissible under the proposed privilege extension. Under the Florida Evidence Code, there is a Husband-Wife Privilege codified as Section 90.504.[158] However, similar to the Texas Spousal Privilege rule,[159] there is no privilege in a criminal proceeding where one of the spouses is charged with committing a crime against the other spouse.[160] Therefore, although the privilege extension should be adopted as a general rule, the communications would not be considered privileged on account of the statutory exception.[161]

There are many other evidentiary issues to be considered including whether, under the Federal Rules of Evidence and those of the applicable

153. *See* Christopher B. Burkett, Note, *"I Call Alexa to the Stand": The Privacy Implications of Anthropomorphizing Virtual Assistants Accompanying Smart-Home Technology*, 20 VAND. J. ENT. & TECH. L. 1181, 1182 (2018) (discussing the pervasive nature of smart-home technology); Stucke & Ezrachi, *supra* note 2, at 1286 ("The Court cited one 2013 poll where 'nearly three-quarters of smartphone users report being within five feet of their phones most of the time, with 12 percent admitting that they even use their phones in the shower.'") (citation omitted).

154. *See* discussion *supra* Section II.

155. *See* discussion *infra* Section IV.

156. *See Alexa, Did He Do It?*, *supra* note 151 ("Police in Florida are investigating whether they have stumbled on a silent witness to a possible murder and are trying to get the truth from 'her.'").

157. *See id.* (putting forth the facts and the unknowns of the tragic Hallandale Beach case).

158. FLA. STAT. ANN. § 90.504 (West 2020).

159. TEX. R. EVID. 504.

160. FLA. STAT. ANN. § 90.504; TEX. R. EVID. 504(b)(1).

161. FLA. STAT. ANN. § 90.504 ; TEX. R. EVID. 504.

state, the proffered evidence from the digital assistant would also (1) be unfairly prejudicial;[162] (2) be inadmissible hearsay;[163] (3) not be able to be properly authenticated;[164] or (4) fail to satisfy the personal knowledge requirement.[165] Furthermore, the prosecution would have to lay the proper foundation for the evidence, including: "the competency of the operator, the fidelity of the recording equipment, the absence of material deletions, additions, or alterations in the relevant portions of the recording, and the identification of the relevant speakers."[166]

F. *The Privilege*

Rule 501 of the Federal and Texas Rules of Evidence discuss legal privileges in general.[167] Federal Rule 501 was codified by Congress in order to give deference to the courts as to what may be construed as legally privileged communications.[168] The current privileges recognized by Texas and federal courts, either by statute, case law, or both, include: required reports privileged,[169] attorney-client privilege,[170] physician-patient privilege,[171] psychotherapist/social worker-client privilege,[172] spousal confidential communication privilege,[173] spousal testimonial privilege,[174] clergyman-penitent privilege,[175] political vote privilege,[176] trade secrets

162. FED. R. EVID. 403; TEX. R. EVID. 403.

163. FED. R. EVID. 801; TEX. R. EVID. 801; FED. R. EVID. 803; TEX. R. EVID. 803; *see* David A. Schlueter, *Hearsay—When Machines Talk*, 53 TEX. B.J. 1135 (1990) (discussing the hearsay implications of machines).

164. FED. R. EVID. 901; TEX. R. EVID. 901.

165. FED. R. EVID. 602; TEX. R. EVID. 602.

166. *See* United States v. Biggins, 551 F.2d 64, 66 (5th Cir. 1977) (providing the foundation for introducing sound recording evidence).

167. FED. R. EVID. 501; TEX. R. EVID. 501.

168. *See* David A. Schlueter, *Do We Need a Parent-Child Privilege?*, 2 CRIM. JUST. 10, 37 (1987) (discussing legal arguments for and against creating new privileges).

169. TEX. R. EVID. 502.

170. FED. R. EVID. 502; TEX. R. EVID. 503.

171. TEX. R. EVID. 509.

172. TEX. R. EVID. 510.

173. TEX. R. EVID. 504(a).

174. TEX. R. EVID. 504(b).

175. TEX. R. EVID. 505.

176. TEX. R. EVID. 506.

privilege,[177] state secrets privilege,[178] and confidential informant privilege.[179] Some jurisdictions have adopted other privileges, such as the parent-child privilege.[180]

Some of the above-mentioned privacy implications were discussed in *"I Call Alexa to the Stand": The Privacy Implications of Anthropomorphizing Virtual Assistants Accompanying Smart-Home Technology*.[181] In a latter portion of the Note, it is suggested courts (1) treat the digital assistants as "persons"[182] and (2) create a new privilege for the digital assistants.[183]

IV. RECOMMENDATIONS

Although the suggestion of a personal assistant privilege[184] is understandable—and even tempting—a slightly different approach should be taken for several reasons. First, despite the Court's ability to honor new privileges,[185] it has been historically reluctant to do so.[186] Creating new privileges can result in a slippery slope and, for this reason, few have been added beyond the original common-law privileges.[187] No independent privilege exists for accountants, but the attorney-client privilege has been

177. TEX. R. EVID. 507.

178. *See generally* Duncan v. Cammell, Laird & Co., A.C. 624 (1942) (detailing the roots of the state secrets privilege in England); *see also* United States v. Reynolds, 345 U.S. 1, 6–7 (1953) (establishing a state secrets privilege in the United States).

179. TEX. R. EVID. 508.

180. *See* Maureen P. O'Sullivan, *An Examination of the State and Federal Courts' Treatment of the Parent-Child Privilege*, 39 CATH. LAW. 201, 202 (1999) (stating the majority of courts do not recognize a parent-child privilege and detailing the various courts' treatment of the privilege).

181. *See generally* Burkett, *supra* note 153, at 1181 (discussing privacy concerns surrounding digital assistants).

182. *See id.* at 1206–10 (stating "[c]ourts have the capacity to define how to treat virtual assistant technology and should extend the term 'person' to certain technologies that are subjected to assignments of agency" and describing various approaches of accomplishing this via either common-law or statutory modification).

183. *See id.* at 1210–16 (suggesting solutions to privacy issues with digital assistants by offering an extensive "privilege between man and machine"—whether under the "instrumental model" or "the humanistic model").

184. *See id.* at 1213 (noting an Alexa-user privilege is necessary to avoid "a chilling effect on communications between these parties, thus defeating the relationship's fundamental purpose.").

185. *See* Trammel v. United States, 445 U.S. 40, 47 (1980) ("The Federal Rules of Evidence acknowledge the authority of the federal courts to continue the evolutionary development of testimonial privileges in federal criminal trials 'governed by the principles of the common law as they may be interpreted . . . in the light of reason and experience.'").

186. *See* Schlueter, *supra* note 168, at 11 (explaining courts generally disfavor evidentiary privileges "because they potentially block otherwise relevant evidence").

187. *See id.* at 37 (weighing the arguments for and against various privileges).

extended to accountants in some circumstances.[188] If a personal assistant privilege were to be created, we might soon have nanny, coworker, and best friend privileges on the horizon. It may initially sound absurd at first read, but it would not be a far stretch to see requests for such privileges emerge if new privileges are created for various relationships.

There are a few ways in which to protect the sanctity of these conversations made in the presence of a virtual assistant:

A. *An Extension of the Existing Privileges*

We should take steps to solve this problem by giving holders and claimants of the respective, existing privileges with the ability to extend the respective, existing privileges to the virtual assistants. The creators of smart home devices have already posited the assistants can be an extension of the user:

> Home. It's more than just four walls and a roof over your head. It's where you feel safest and most comfortable. But what if your home knew you as well as you know it? What if it could recognize you, and anticipate your needs? . . . What if your home became—in small ways, then big ones—an extension of you?[189]

This recommendation seeks to prevent virtual assistants from effectively "testifying" as to what was heard and recorded. This could either be accomplished by the Court adopting this method of analysis at common-law, by the Rules regarding privilege to be updated individually to reflect the same, or by the Rules Committee adding another Rule which would limit the former by this new exception.

The basic premise of this proposal is neither unheard of nor unprecedented.[190] As mentioned, the attorney-client privilege has been extended to accountants in some circumstances.[191] Translators are

188. *See generally* United States v. Kovel, 296 F.2d 918 (2d Cir. 1961) (extending the attorney-client privilege to accountants hired by the attorney or client under certain circumstances).

189. Ryan G. Bishop, Note, *The Walls Have Ears . . . and Eyes . . . and Noses: Home Smart Devices and the Fourth Amendment*, 61 ARIZ. L. REV. 667, 667 (2019) (quoting a portion of the Nest smart home website which is no longer published).

190. *See generally* Hawkins v. United States, 358 U.S. 74 (1958) (reiterating the common-law rule preventing spouses from testifying against one another); *see also* Stein v. Bowman, 38 U.S. 209, 223 (1839) (holding a wife could not testify against her husband even though he had died).

191. *See Kovel*, 296 F.2d at 922 ("Hence the presence of an accountant, whether hired by the lawyer or by the client, while the client is relating a complicated tax story to the lawyer, ought not

permitted to be present during privileged conversations without violating the privilege,[192] as are employees of attorneys and doctors[193] under the proper circumstances. For generations, husbands and wives were prohibited from testifying against their respective spouses,[194] they were considered legally incompetent to do so.[195] The common-law reasoning was for the sake of "fostering the harmony and sanctity of the marriage relationship."[196] After all—as romantically phrased by the Supreme Court in *Stein v. Bowman*—marriage has long been considered "the best solace of human existence."[197]

In *Trammel v. United States*,[198] the tides turned and spouses have since been allowed to testify against one another if they so choose.[199] The reasoning behind this decision largely fell on the argument that the spousal "relationship is almost certainly in disrepair [if one spouse would testify against the other]; there is probably little in the way of marital harmony for

destroy the privilege, . . . the presence of the accountant is necessary, or at least highly useful, for the effective consultation between the client and the lawyer which the privilege is designed to permit.").

192. *See id.* at 921 (explaining several situations in which attorneys may have linguists present to best assist a client).

193. *See id.* ("On the other hand, in contrast to the Tudor times when the privilege was first recognized, . . . the complexities of modern existence prevent attorneys from effectively handling clients' affairs without the help of others; few lawyers could now practice without the assistance of secretaries, file clerks, telephone operators, messengers, clerks not yet admitted to the bar, and aides of other sorts. 'The assistance of these agents being indispensable to his work and the communications of the client being often necessarily committed to them by the attorney or by the client himself, the privilege must include all the persons who act as the attorney's agents.'" (quoting 8 Wigmore, Evidence, § 2301; Annot., 53 A.L.R. 369 (1928))) (internal citation omitted).

194. *Hawkins*, 358 U.S. at 75.

195. *See id.* ("The common-law rule, accepted at an early date as controlling in this country, was that husband and wife were incompetent as witnesses for or against each other."); *Stein*, 38 U.S. at 222–23 ("And it is conceived that this principle [of spousal incompetency to testify against one another in court] does not merely afford protection to the husband and wife, which they are at liberty to invoke or not, at their discretion, when the question is propounded; but it renders them incompetent to disclose facts in evidence in violation of the rule. And it is well that the principle does not rest on the discretion of the parties. If it did, in most instances it would afford no substantial protection to persons uninstructed in their rights, and thrown off their guard and embarrassed by searching interrogatories.").

196. Trammel v. United States, 445 U.S. 40, 44 (1980).

197. *Stein*, 38 U.S. at 223.

198. *Trammel*, 445 U.S. at 40.

199. *See id.* at 53 ("Accordingly, we conclude that the existing rule should be modified so that the witness-spouse alone has a privilege to refuse to testify adversely; the witness may be neither compelled to testify nor foreclosed from testifying. This modification—vesting the privilege in the witness-spouse—furthers the important public interest in marital harmony without unduly burdening legitimate law enforcement needs.").

the privilege to preserve."[200] However, this sad circumstance[201] is not applicable with regard to the above examples of testimony by the virtual assistants. In the virtual assistant scenarios mentioned, the claimants and holders of the various privileges do not seek to violate one another's confidence. So why should we allow six-inch tall towers or rectangular prisms in our pockets to be forced to disclose these privileged conversations? We should not. If individuals seek to uphold the privileges granted them by common-law or the Texas and Federal Rules of Evidence, Alexa should not stand in their way.

By taking this initiative, the Court could avoid creating a new privilege, as is its preference,[202] yet enable people engaging in otherwise privileged speech to feel comfortable around smart speakers. This would promote further technological advancement rather than fear of the same:

> As Justice Brandeis explained in his famous dissent, the Court is obligated—as "[s]ubtler and more far-reaching means of invading privacy have become available to the Government"—to ensure that the "progress of science" does not erode Fourth Amendment protections.[203]

Undoubtedly, privacy is not absolute, as "the government is permitted to limit that interest if it can demonstrate a compelling government interest and that its means of limitation or intrusion are necessary and closely tailored to meeting that interest."[204] However, privileged conversations, such as pillow talk between spouses and confidential discussions between attorneys and their clients or doctors and their patients, should not be at risk.[205]

B. *Creating a "Castle" Privilege?*

Should the Court be open to the idea of creating a new privilege in addition to prohibiting the virtual assistants from testifying as mentioned

200. *Id.* at 52.

201. *See id.* (noting the marriage was already in such a state of disrepair since Trammel's wife was willing to testify against him in exchange for lenient treatment).

202. *See* Schlueter, *supra* note 168, at 11 (stating "the general principle that evidentiary privileges are generally disfavored").

203. Carpenter v. United States, 138 S. Ct. 2206, 2223 (quoting Olmstead v. United States, 277 U.S. 438, 473–74 (1928) (Brandeis, J., dissenting)).

204. *See* Schlueter, *supra* note 168, at 13 (illuminating flaws in the syllogism adopted by proponents of the parent-child privilege).

205. *See* discussion *supra* Section IV(A).

above,[206] the Court should create a so-called "castle" privilege. The proposed title to this privilege was inspired by the following quote by Sir Edward Coke: "every man's house is his castle, and he ought to keep and defend it at his peril; and if any one be robbed in his house, it shall be esteemed his own default and negligence."[207]

I propose this castle privilege would only protect recordings within the home in circumstances where one has a legitimate expectation of privacy. Specifically, it would not apply in the home if individuals other than one's spouse were present since one would have no legitimate expectation of privacy under these circumstances. Circumstances in which the speech would be protected by the castle privilege, were it to be adopted, would include when the individual was at home, speaking aloud—whether to the personal assistant intentionally or if the assistant was recording unbeknownst to the individual.

This is likewise not unprecedented. Looking back at *Kyllo v. United States*, any information obtained from within the home which would ordinarily not have been accessible without physical intrusion, or without technology not in general public use, constituted a search.[208] Although many people now have at least one virtual assistant,[209] it is the smart device itself that is available to the general public[210]—not the remote listening and recording, or subsequent cloud transmission and cloud verification technologies. The castle privilege would be consistent under *Kyllo*[211] but would extend explicitly to the virtual assistants.

206. *See* discussion *supra* Section IV(A).

207. *Castle Doctrine*, THE WOLTERS KLUWER BOUVIER LAW DICTIONARY (10th ed. 2014).

208. *See generally* Kyllo v. United States, 533 U.S. 27 (2001).

209. *See* CHRISTI OLSON & KELLI KEMERY, MICROSOFT, VOICE REPORT FROM ANSWERS TO ACTION: CUSTOMER ADOPTION OF VOICE TECHNOLOGY AND DIGITAL ASSISTANTS 14 (2019), https://advertiseonbing-blob.azureedge.net/blob/bingads/media/insight/whitepapers/2019/04%20apr/voice-report/bingads_2019_voicereport.pdf [https://perma.cc/H9SY-YTVF] ("Gartner predicts that by 2020, 75% of households will have at least one smart speaker. By January 2019, we saw that 45% already now own a smart speaker. For many survey respondents, one was not enough. 41% of respondents who own a smart speaker already have multiple speakers (2+)") (footnote omitted).

210. *See id.* at 15 (reminding us it is important to remember "[t]his is just the beginning" and even "voice and digital assistants are still in very early stages of adoption").

211. *See generally* Kyllo v. United States, 533 U.S. 27 (2001).

V. CONCLUSION

Therefore, the existing privileges should be extended to the digital assistants—based on a lack of competency as was rooted in common law for public policy reasons—and a "castle" privilege should exist in a person's home when she has a legitimate and reasonable expectation of privacy.[212]

The aforementioned issues are becoming ever more prevalent as digital assistants are nearly unavoidable.[213] A digital assistant could be lurking in the pocket of someone you are talking to, in a business office you visit, or in a conference room during a *supposedly* confidential proceeding.[214] Given the imperfection of the waking or activation technology, these devices may be triggered inadvertently and send privileged and private conversations to the cloud for review by Amazon workers if the setting is not disabled.[215] For these reasons and more, current lack of protection and privacy in the presence of the digital assistants is something we can no longer tolerate.

Their present ability to disclose privileged conversations[216] is contrary to the reasoning behind privileges in the state and Federal Rules of Evidence. Even in the most severe criminal cases, compelling one spouse to testify against the other is forbidden, with just a few exceptions,[217] because it is deemed to be in the interest of public policy to promote the institution of marriage.[218] Digital assistants should not have the ability, nor the privilege, to disclose these privileged conversations.

---

212. *See* discussion *supra* Sections IV(A); *see* discussion *supra* Sections II(B).

213. *See* discussion *supra* Sections II–IV. *See generally* OLSON & KEMERY, *supra* note 209 (evaluating "customer adoption of voice technology and digital assistants").

214. *See generally* Ian Samuel, *The New Writs of Assistance*, 86 FORDHAM L. REV. 2873, 2884–85 (2018) (illustrating how virtual assistants are becoming more widely used, both in the professional world and in private use).

215. *See Manage Your Alexa Privacy Settings, Manage Your Alexa Data*, AMAZON (2019), https://www.amazon.com/gp/help/customer/display.html?nodeId=GPGRYRZ494GDFPZ2 [https://perma.cc/5G37-KGAA] (instructing how to prevent Amazon employees' manual review of recordings).

216. *See* Hosey, *supra* note 11, at 59 ("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.").

217. *See* TEX. R. EVID. 504; Stein v. Bowman, 38 U.S. 209, 217 (1839) ("This rule is subject to some exceptions, as when the husband commits an offence against the person of his wife.").

218. *See* Hawkins v. United States, 358 U.S. 74, 78 (1958) ("Adverse testimony given in criminal proceedings would, we think, be likely to destroy almost any marriage."); *Stein*, 38 U.S. at 223 (forbidding a widow from testifying against her then-deceased husband).