BETWEEN YOU, ME, AND ALEXA: ON THE LEGALITY OF VIRTUAL ASSISTANT DEVICES IN TWO-PARTY CONSENT STATES

Ria Kuruvilla*

Abstract: When an Amazon Echo is activated, the device is constantly recording and sending those recordings to Amazon's cloud. For an always recording device such as the Echo, getting consent from every person subject to a recording proves difficult. An Echo-owner consents to the recordings when they purchase and register the device, but when does a guest in an Echo-owner's home consent to being recorded?

This Comment uses Amazon's Echo and Washington's privacy statute to illustrate the tension between speech-activated devices and two-party consent laws—which require that all parties subject to a recording consent to being recorded. This Comment argues that the Washington State Legislature should enact a statute that mirrors the Anti-Eavesdropping Act and carve out a civil cause of action against manufacturers of speech-activated devices for individuals that are harmed by violations of the two-party consent law.

INTRODUCTION

A family in Portland, Oregon received a disturbing phone call. The voice on the line said, "[u]nplug your Alexa devices right now . . . [y]ou're being hacked."[1] The call was from one of the husband's employees who lived in Seattle, Washington, Amazon's headquarters.[2] Without being prompted and without permission, the family's Amazon Echo device had recorded a conversation between the husband and wife and sent it to the employee.[3]

Speech-activated devices with virtual assistants such as Amazon's Echo can be incredibly helpful. They can increase efficiency by managing schedules, simplifying tasks like ordering groceries, and easing the lives

* J.D. Candidate, University of Washington School of Law, Class of 2020. I would like to thank Professors Ryan Calo and Steve Calandrillo for their guidance and contributions. I would also like to thank the fantastic members of *Washington Law Review*, without whom this piece would not be possible.

1. Hamza Shaban, *An Amazon Echo Recorded a Family's Conversation, Then Sent it to a Random Person in Their Contacts, Report Says*, WASH. POST (May 24, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/05/24/an-amazon-echo-recorded-a-familys-conversation-then-sent-it-to-a-random-person-in-their-contacts-report-says/?utm_term=.6efce18494f9 [https://perma.cc/F3QP-2DJP].

2. *Id.*

3. Niraj Chokshi, *Is Alexa Listening? Amazon Echo Sent Out Recording of Couple's Conversation*, N.Y. TIMES (May 25, 2018), https://www.nytimes.com/2018/05/25/business/amazon-alexa-conversation-shared-echo.html [https://perma.cc/LZ65-ACA2].

of people with disabilities. However, as evidenced by this Portland family, the conveniences that come with virtual assistants inevitably give rise to privacy concerns.

Imagine two friends having a private conversation in an Echo-owner's home. The Echo is on, playing music, and recording while the friends are catching up. One friend tells the other an off-hand joke, admits to a crime, or reveals their sexual preferences. Suddenly, personal, sensitive information is recorded and sent to Amazon's cloud—information that Amazon might listen to or inadvertently release. But the friend never consented to the recording. The friend might not even know that the device is in the room.

Such situations show a tension between speech-activated devices and two-party consent laws, which require the consent of all parties to a conversation prior to recording.[4] This conflict gives rise to several questions: what happens when an Echo records the private conversation of someone other than the owner? If a guest asks the Echo a question, did the guest consent to having their conversation recorded? How should Amazon get the consent of that guest? Should the Echo-owner be responsible for getting consent? Should Amazon?

This Comment uses Washington State's caselaw to explore these questions and to illustrate how Amazon's Echo interacts with Washington's two-party consent law. In particular, this Comment argues that recordings by speech-activated devices violate the two-party consent doctrine and that the Washington State Legislature should address privacy risks proactively by creating a cause of action against manufacturers of such devices and by forming an Act that mirrors the Anti-Eavesdropping Act.[5] By clarifying who the onus falls on for accidental, surreptitious recordings, the Washington State Legislature can ensure that individuals privacy rights are protected and that the manufacturers of speech-activated devices are being held accountable for violations.

Part I describes speech-activated devices and virtual assistants in general, how Amazon's Echo and its Alexa technology works, and the ways in which data collected by the technology is handled. Part II demonstrates situations where recordings by speech-activated devices present risks to consumers' privacy rights. Part III describes relevant federal law and details Washington's two-party consent law[6] and the case law surrounding it. Part IV considers how speech-activated devices apply to Washington's two-party consent law. Part V describes the shortcomings of proposed solutions and suggests an alternative solution

4. WASH. REV. CODE § 9.73.050 (2019).

5. Assemb. Bill 1395, 2019 Leg., 2019–2020 Sess. (Cal. 2019).

6. WASH. REV. CODE § 9.73.050.

to the conflict. Namely, that the Washington State Legislature should create both an act that mirrors the Anti-Eavesdropping Act and a cause of action against the manufacturer of speech-activated devices for violations of the statute.

I. VIRTUAL ASSISTANTS AND SPEECH-ACTIVATED DEVICES

Virtual assistants such as Amazon's "Alexa," Apple's "Siri," and Microsoft's "Cortana," which are integrated into speech-activated devices, have become increasingly popular.[7] The global intelligent virtual assistant market reached $2.3 billion in 2018 and is expected to increase to $19.6 billion by 2025.[8] Researchers predict that 75% of households will have intelligent virtual assistants by 2020.[9]

While many companies have developed virtual assistants, Amazon's Alexa leads the pack.[10] Alexa was released in November 2014, twenty-eight years after the most recent amendment to Washington's two-party consent law.[11] Since then, Alexa's popularity has only grown. In 2018 alone, both the number of Echo-owners and the number of daily Alexa interactions doubled.[12] The virtual assistant, Alexa, can be found in more

---

7. When referring to the speech-activated device, this Comment will use the term "Echo." When referring to the virtual assistant integrated into the device, this Comment will use the term "Alexa."

8. Zion Market Research, *Global Intelligent Virtual Assistant Market Will Reach USD 19.6 Billion by 2025: Zion Market Research*, GLOBENEWSWIRE (January 25, 2019), https://www.globenewswire.com/news-release/2019/01/25/1705456/0/en/Global-Intelligent-Virtual-Assistant-Market-Will-Reach-USD-19-6-Billion-By-2025-Zion-Market-Research.html [https://perma.cc/9YSP-WVC3].

9. Bret Kinsella, *Gartner Predicts 75% of US Households Will Have Smart Speakers by 2020*, VOICEBOT.AI (Apr. 14, 2017), https://voicebot.ai/2017/04/14/gartner-predicts-75-us-households-will-smart-speakers-2020/ [https://perma.cc/CY2H-S3SF].

10. Adam Heitzman, *How Popular is Voice Search?,* HIGHERVISIBILITY.COM (Jan. 1, 2019), https://www.highervisibility.com/blog/how-popular-is-voice-search/ [https://perma.cc/8QJC-MPWN]; Bret Kinsella, *U.S. Smart Speaker Market Share: Apple Debuts at 4.1%, Amazon Falls 10 Points and Google Rises*, VOICEBOT.AI (Jun. 3, 2018), https://voicebot.ai/2018/06/03/u-s-smart-speaker-market-share-apple-debuts-at-4-1-amazon-falls-10-points-and-google-rises/ [https://perma.cc/4PR4-2BNN]; David Pierce, *Alexa Just Conquered CES. The World Is Next*, WIRED (Jan. 6, 2017), https://www.wired.com/2017/01/ces-alexa-in-everything/ [https://perma.cc/4UP6-UERQ]; Greg Sterling, *Survey: Alexa the Most Frequently Used Assistant, Cortana Seen as Most Accurate*, SEARCH ENGINE LAND (Feb. 9, 2017), https://searchengineland.com/survey-alexa-frequently-used-assistant-cortana-seen-accurate-269052 [https://perma.cc/QN7L-39F3].

11. Darrell Etherington, *Amazon Echo Is a $199 Connected Speaker Packing an Always-On Siri-Style Assistant***,** TECHCRUNCH (Nov. 6, 2014), https://techcrunch.com/2014/11/06/amazon-echo/ [https://perma.cc/8GY4-CTAL]; *see also* WASH. REV. CODE § 9.73.050 (2018).

12. Toni Reid, *Everything Alexa Learned in 2018*, DAYONE: THE AMAZON BLOG (Dec. 19, 2018)

than just the Echo device; it can also be found in thermostats, televisions, security systems, and vacuums.[13] In January 2019, Amazon reported that over 100 million devices with Alexa had been sold.[14]

And Amazon has no plans to slow down. Alexa can already be found in some cars[15] and hotels,[16] and Amazon has plans to have Alexa in even more devices and places.[17] For example, Amazon recently partnered with Marriott and the Wynn hotel in Las Vegas to put them in hotel rooms.[18] Amazon also announced a deal with Toyota, one of the world's largest auto manufacturers,[19] which will integrate Alexa into all of its cars.[20]

A. Overview of Alexa and the Echo

To set up an Alexa virtual assistant, an individual needs an Alexa-enabled device such as the Echo, a wifi connection, an Amazon account, and the Alexa app installed on a smartphone or tablet.[21] Once an Alexa app is paired to an Alexa-enabled device, anyone can use the device, including those without an Amazon account.[22]

Users can ask Alexa to call friends, play music, or add an event to their calendar.[23] To complete these tasks, Alexa uses "speech recognition technology," defined by the technology sector as the "ability to speak naturally and contextually with a computer system in order to execute

---

https://blog.aboutamazon.com/devices/everything-alexa-learned-in-2018 [https://perma.cc/ALG4-HFN2].

13. *Smart Home,* AMAZON, https://www.amazon.com/b?node=6563140011 [https://perma.cc/ER72-KB36].

14 Lucas Matney, *More than 100 Million Alexa Devices Have Been Sold* ,TECH CRUNCH (Jan. 4, 2019), https://techcrunch.com/2019/01/04/more-than-100-million-alexa-devices-have-been-sold/ [https://perma.cc/L2VC-7PGB].

15. Karen Hao, *Amazon Is Bringing Alexa to Your Toyota,* QUARTZ (Jan. 10, 2018), https://qz.com/1176558/amazons-alexa-is-coming-to-your-toyota/ [https://perma.cc/VE2W-G3H3].

16. Raphael Davidian, *Alexa and Third Parties' Reasonable Expectation of Privacy*, 54 AM. CRIM. L. REV. ONLINE 58, 60 (2017).

17. Reid, *supra* note 10.

18. Chris Welch, *The Wynn Las Vegas Is Putting an Amazon Echo in Every Hotel Room***,** VERGE: CIRCUIT BREAKER (Dec. 14, 2016), https://www.theverge.com/circuitbreaker/2016/12/14/13955878/wynn-las-vegas-amazon-echo-hotel-room-privacy [https://perma.cc/5W2B-DH2V].

19. Hao, *supra* note 15.

20. Notably, it is not clear whether the option of reviewing and deleting voice recordings would be available to every hotel guest. *Id.*; *see also infra* note 121.

21. Erika Raws & Tyler Lacoma, *How to Set Up an Amazon Echo*, DIGITAL TRENDS (July 13, 2019), https://www.digitaltrends.com/home/how-to-set-up-your-amazon-echo/ [https://perma.cc/SP52-ZBBV].

22. *Id.*

23. *Alexa and Alexa Device FAQs,* AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=201602230 [https://perma.cc/P75S-7BL6].

commands or dictate language."[24] Put more simply, a user can say to Alexa, "Alexa, call grandma; Alexa, dim the lights; Alexa, add tomatoes to my shopping list," and Alexa will execute the command.[25]

Alexa's speech recognition technology also allows it to be natural, personal, and conversational.[26] For example, Alexa communicates with users in a human-simulated voice. In 2018, Amazon reported that Alexa told more than 100 million jokes.[27] Now, with its new whisper mode, Alexa can detect if a user is whispering and will whisper back.[28]

The Echo is a speech-activated device, meaning that it is "listening" for a wake word, such as "Alexa" or "Echo."[29] More specifically, the device is constantly analyzing temporary voice recordings to detect the wake word and deleting those voice recordings if the wake word is not detected.[30] When the device detects the wake word, it begins to record everything it hears.[31] It then transmits those recordings and data to the cloud for storage.[32] Notably, it is common for a device to accidentally begin recording because it mishears the wake word.[33]

When an Echo is recording, the light ring on it becomes blue.[34] The light ring turns others colors depending on its current state and function: blue, orange, red, yellow, red, green, white, or purple.[35] For example, orange means connecting to wifi, green indicates an incoming call, and

---

24. STACEY GRAY, ALWAYS ON: PRIVACY IMPLICATIONS OF MICROPHONE-ENABLED DEVICES (Future of Privacy Forum ed., 2016), https://fpf.org/wpcontent/uploads/2016/04/FPF_Always_On_WP.pdf [https://perma.cc/E28M-M6EV].

25. *Alexa and Alexa Device FAQs*, *supra* note 23.

26. Reid, *supra* note 12.

27. *See id.*

28. *See id.*

29. GRAY, *supra* note 24.

30. *Enable Cloud-Based Wake Word Verification*, AMAZON, https://developer.amazon.com/docs/alexa- voice-service/enable-cloud-based-wake-word-verification.html (last visited Oct. 5, 2019).

31. *Alexa and Alexa Device FAQs, supra* note 23.

32. *Id.*

33. 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 [https://perma.cc/D9GT-UBSQ]; Geoffrey A. Fowler, *Hey Alexa, Come Clean About How Much You're Really Recording Us*, THE WASHINGTON POST (May 24, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/05/24/hey-alexa-come-clean-about-how-much-youre-really-recording-us/?noredirect=on&utm_term=.58172d3165cd [https://perma.cc/SNB2-C4FU].

34. *About the Light* Ring, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=201601790 [https://perma.cc/WCJ5-A3PY]. Amazon does not provide this information in their Echo FAQs but does on a separate information page. *Id.*

35. *Id.*

red represents a disabled microphone.[36]

Amazon uses these recordings for many purposes—primarily to improve and personalize a user's experience by adapting to speech patterns, vocabulary, and personal preferences.[37] For example, by keeping track of the songs that a user asks Alexa to play, the technology can better choose what songs to play when the user says, "Alexa, play music."[38] The technology also has the ability to recognize different voices and can provide a personalized experience for each individual user.[39]

Amazon can also use this data to better other users' experiences.[40] For example, the device currently understands the "nonaccent" of white, American, nonimmigrant voices best.[41] When other voices were tested, the tests often resulted in errors, strange responses, and apologies from Alexa.[42] By analyzing these recordings, the device can learn to better understand a diverse array of voices and accents.[43]

B. How Amazon handles data compared to Apple and Google

Speech-activated devices from Amazon, Google, and Apple all begin recording when they hear their wake word and store data to improve performance.[44] However, the companies differ in how they review data, what personal information they collect, and how they delete data.

To improve Alexa's capabilities, Amazon employs thousands of people around the world to review voice recordings captured by Echo devices.[45] These employees listen to the recordings, transcribe them, annotate them,

---

36. *Id.*

37. *Alexa and Alexa Device FAQs, supra* note 23.

38. *Id.*

39. Chris Welch, *Amazon's Alexa Can Now Recognize Different Voices and Give Personalized Responses*, VERGE: CIR. BREAKER (Oct. 11, 2017), https://www.theverge.com/circuitbreaker/2017/10/11/16460120/amazon-echo-multi-user-voice-new-feature [http://perma.cc/4B4F-H2G9].

40. *Alexa and Alexa Device FAQs, supra* note 23.

41. Drew Harwell, *The Accent Gap*, WASH. POST (Jul. 19, 2018), https://www.washingtonpost.com/graphics/2018/business/alexa-does-not-understand-your accent/?utm_term=.7eac62088cd7 [https://perma.cc/J5PV-QLMB].

42. *Id.*

43. *Alexa and Alexa Device FAQs, supra* note 23.

44. Lisa Eadicicco, *Amazon Workers Reportedly Listen to What You Tell Alexa — Here's How Apple and Google Handle What You Say to Their Voice Assistants*, BUSINESS INSIDER (Apr. 15, 2019), https://www.businessinsider.com/how-amazon-apple-google-handle-alexa-siri-voice-data-2019-4 [https://perma.cc/GY2M-P7GC].

45. Matt Day, Giles Turner, & Natali Drozdiak, *Amazon Workers Are Listening to What You Tell Alexa*, BLOOMBERG (April 10, 2019), https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio [https://perma.cc/6X8R-N2NX].

and feed them back into the software.[46] Each employee reviews as many as 1,000 audio clips a day and transcribes everything a device picks up, even background conversations.[47]

When employees need assistance in determining what a recording says or they come across a particularly amusing recording, they share clips in internal chatrooms.[48] While clips often involve ordinary information, the listeners sometimes overhear information that users would rather keep private.[49] For example, the employees have overheard recordings of possible criminal conduct, such as sexual assault.[50] When the employees overhear disturbing clips such as these, they share them in the internal chat rooms for support.[51]

Although reviewers do not see a user's full name and address, the recordings are associated with an account number, the user's first name, and the device's serial number.[52] Amazon generally keeps the recordings indefinitely, but a user can choose to review and delete voice recordings associated with their account.[53] However, Amazon states that deleting recordings does not necessarily delete any of the messages sent and received through Alexa.[54] Additionally, Amazon claims that, by deleting voice recordings, a user's Alexa experience might be "degraded."[55]

In contrast, when a user asks Apple's "Siri" a question, the information is tied to a random identifier generated by the device that can be reset at any time.[56] Consequently, the data sent to Apple is not associated with an Apple ID account.[57] Like Amazon, Apple saves recordings to develop Siri, but Apple only saves the voice recordings with the identifier for six months and then deletes the data.[58] Apple sometimes saves another copy of the data to continue to improve Siri's performance, but that data is randomized and not connected to any identifier at all.[59]

---

46. *Id.*
47. *Id.*
48. *Id.*
49. *Id.*
50. *Id.*
51. *Id.*
52. *Id.*
53. *Alexa and Alexa Device FAQs*, *supra* note 23.
54. *Id.*
55. *Id.*
56. Eadicicco, *supra* note 44.
57. *Id.*
58. *Id.*
59. *Id.*

Google also has a manual review system for recordings but states that the process only applies to a "fraction" of recordings.[60] Google Home users can opt out, review, and delete those recordings.[61] A Google Home user can also adjust their settings so that the device does not record anything it hears after the wake word.[62] However, in contrast to Amazon, Google's audio recordings are not associated with personally identifiable information, thus providing a level of protection that Amazon does not.[63]

Amazon only annotates a small sample of recordings captured by Echo devices and an Amazon spokesperson stated that Amazon takes the privacy of customer's information seriously.[64] Still, the idea of Amazon employees listening and transcribing every word of a private conversation is unsettling. In fact, reviewers have stated that Amazon users often ask, "Alexa, is someone else listening to us?"[65]

C. How Amazon Gets Consent

Amazon is required to gain an owner's consent before they interact with Alexa.[66] Generally, companies do this with a terms of service agreement or by including a disclaimer with the product.[67] In accordance with this requirement, an individual that registers an Echo device agrees to Alexa's Terms of Use and Amazon's Conditions of Use, although non-registered users can still interact freely with the devices.[68]

Amazon's Conditions of Use state, "You are responsible for maintaining the confidentiality of your account and password and for restricting access to your account, and you agree to accept responsibility for all activities that occur under your account or password."[69] More specific to recording, Alexa's Terms of Use provide that "Alexa streams

---

60. *Id.*

61. *Id.*

62. Geoffrey A. Fowler, *Alexa Has Been Eavesdropping on You this Whole Time*, THE WASH. POST (May 6, 2019), https://www.washingtonpost.com/technology/2019/05/06/alexa-has-been-eavesdropping-you-this-whole-time/?utm_term=.75c56e8e5568 [https://perma.cc/7B55-6RRP].

63. Eadicicco, *supra* note 44.

64. Day, Turner, & Drozdiak, *supra* note 45.

65. *Id.*

66. Allison S. Bohm et. al., *Privacy and Liberty in an Always-On, Always-Listening World*, 19 COLUM. SCI. & TECH. L. REV. 1, 19 (2017).

67. *Id.*

68. Report and Recommendation at 3, B.F. & A.A. v. Amazon, No. C19-910-RAJ-MLP (W.D. Wash. Oct. 21, 2019).

69. *Amazon Conditions of Use,* AMAZON, https://www.amazon.com/gp/help/customer/display.html?ie=UTF8&%2AVersion%2A=1&%2Aentries%2A=0&nodeId=508088 [https://perma.cc/NNK6-P2P9].

audio to the cloud when you interact with Alexa. Amazon processes and retains your Alexa Interactions . . . " and that "[b]y using Alexa, you agree to be bound by the terms of this Agreement."[70] Basically, by using Alexa, "you" consent to have your conversations recorded and stored in Amazon's cloud.[71]

It is unclear whether Amazon is attempting to gain the consent of a device owner, everyone in a household, or anyone that might be using the device by using the term "you."[72] One critic argues that the language is overly broad and that it is unlikely that terms of service could even be designed to bind everyone in a household.[73] Regardless of whether the terms bind members of a household, most guests to a device-owner's home will not have seen or agreed to Amazon's Conditions of Use or Alexa's Terms of use and thus will not have consented explicitly under Washington law.[74] For those individuals that have not provided consent to being recorded by the Echo, potential violations of two-party consent laws arise, and individuals' privacy rights are put at risk.

Even Google's devices chief recognizes these concerns.[75] When asked about making guests aware of virtual assistant devices recording, he stated "[i]t's quite important for all these technologies to think about all users . . . we have to consider all stakeholders that might be in proximity."[76] He further provided, "Does 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."[77]

II. RISKS ASSOCIATED WITH THE ECHO'S RECORDING CAPABILITIES

There are various risks associated with the Echo's recording function. For example, the device can invade individuals' privacy rights by recording and transcribing personal and sensitive information. Not only can it retain the recordings, but it can also inadvertently send them out.

---

70. *Id.*

71. *Id.*

72. Tom McKay, *Lawsuits Claim Amazon's Alexa Voice Assistant Illegally Records Children without Consent,* GIZMODO (July 12, 2019), https://gizmodo.com/lawsuits-claim-amazons-alexa-voice-assistant-illegally-1835468920 [https://perma.cc/HA88-XS59].

73. *Id.*

74. *See infra* Part IV.

75. 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 [https://perma.cc/B5F5-8K46].

76. *Id.*

77. *Id.*

Moreover, the information it gathers can be used by Amazon without consent—for example, to advertise or to sell to third parties.

A. Amazon Inadvertently Sends Out Recordings of Alexa Interactions

There have been two incident reports in recent times where Amazon inadvertently sent the recordings of a user to a stranger.[78] First, when a user in Germany requested his archive of recordings from Amazon he ended up receiving 1,700 audio files from a person whom he did not know.[79] In a statement, Amazon told the *Washington Post*,[80] "[t]his was an unfortunate case of human error and an isolated incident."[81] Although Amazon claims this was a one-time occurrence, the incident illustrates the risk of Amazon inadvertently releasing recordings with sensitive information.

As described earlier, the second incident occurred when an Echo device inadvertently sent a recording of a conversation between a husband and his wife to one of the man's employees.[82] The wife said that the Alexa never asked her permission to send the conversation.[83] In a responding statement, Amazon said,

> Echo woke up due to a word in background conversation sounding like "Alexa," . . . . Then, the subsequent conversation was heard as a "send message" request. At which point, Alexa said out loud "To whom?" At which point, the background conversation was interpreted as a name in the customer's contact list. Alexa then asked out loud, "[contact name], right?" Alexa then interpreted background conversation as "right". As unlikely as this string of events is, we are evaluating options to make this case even less likely.[84]

Although Amazon claimed it was an unlikely series of events, the family disconnected their devices and is currently seeking a refund from Amazon.[85] The wife told a local news station, "I'm never plugging that

---

78. Shaban, *supra* note 1; Hamza Shaban, *Amazon Alexa user receives 1,700 audio recordings of a stranger through 'human error'*, (Dec. 20, 2018, 7:10 AM), https://www.washingtonpost.com/technology/2018/12/20/amazon-alexa-user-receives-audio-recordings-stranger-through-human-error/ [https://perma.cc/DX3Y-2LP4] [hereinafter Shaban, *Amazon Alexa user recieves 1,700 audio recordings*].

79. Shaban, *Amazon Alexa user recieves 1,700 audio recordings*, *supra* note 78.

80. Ironically, Jeff Bezos owns the Washington Post. *Id.*

81. *Id.*

82. Shaban, *supra* note 1.

83. Chokshi, *supra* note 3.

84. *Id.*

85. *Id.*

device in again, . . . I can't trust it."[86] Because this recording was sent to someone the family knew, the husband's employee, rather than a stranger, it is easy to see how the incident could have been much more damaging. If the conversation had contained private information, the employee could have chosen to reveal it at the husband's workplace which might cause harm to his business reputation.

B. Alexa Overhears a Murder in Arkansas

Beyond the implications for the privacy rights of Echo-owners, Alexa recordings can have implications for criminal investigations. In 2015, in Bentonville, Arkansas, Victor Collins was found dead in the hot tub of James Bates' home.[87] Bates had invited two men over, including Collins, to drink beer and to watch football.[88] Bates claimed he went to bed around 1:00 am and that he found Collins dead in his hot tub when he woke up.[89] Collins had a high blood alcohol content, .32, Bates' attorney said Collins' death was a tragic accident resulting from Collins' binge drinking.[90] However, investigators found signs of struggle and indications that the patio and hot tub had been hosed down before police arrived, eliciting further investigation.[91]

Amazon's recordings came into play when one of the people present on the night of Bates' death remembered that they had heard music streaming through an Echo that evening.[92] The prosecutor's office requested Amazon hand over any data recorded that night two different times, but Amazon pushed back.[93] In a statement sent to CNN, Amazon said, "Amazon will not release customer information without a valid and binding legal demand properly served on us . . . . Amazon objects to overbroad or otherwise inappropriate demands as a matter of course."[94] In a later memo, Amazon's lawyers wrote, "[g]iven the important First Amendment and privacy implications at stake, the warrant should be

86. *Id.*

87. Elliot C. McLaughlin and Keith Allen, *Alexa, Can You Help with this Murder Case?,* CNN (Dec. 28, 2016), https://www.cnn.com/2016/12/28/tech/amazon-echo-alexa-bentonville-arkansas-murder-case-trnd/ [https://perma.cc/53LA-MFN5].

88. *Id.*

89. *Id.*

90. *Id.*

91. *Id.*

92. *Id.*

93. *Id.*

94. *Id.*

quashed unless the Court finds that the State has met its heightened burden for compelled production of such materials."[95]

Eventually, Bates agreed to have the data from the device handed over to the prosecutor's office and Amazon was not forced to hand it over on their own.[96] Amazon handed over Bates' account details and purchases, and police say they were able to pull some data off of the speaker, but it remains unclear what information they gained access to.[97]

While the issue never reached a court, existing statutes do not address whether Amazon would have been able to release the information without Bates's consent.[98] As outlined below, both of these situations could violate RCW 9.73.030[99] if they occurred in Washington.[100] And as Washington's privacy statute is written, the victims would not have clear legal recourse against Amazon.

III. WIRETAPPING LAWS

Although speech-activated devices raise consumer privacy issues, the devices remain largely unregulated at the federal level.[101] Commercial privacy laws, such as the Electronics Communications Privacy Act that created amendments to the Wiretap Act,[102] do not fully address the information collected by speech-activated devices.[103] In particular, the Wiretap Act[104] only prohibits intentionally intercepting "any wire, oral, or electronic communication" without consent of at least one of the parties to the recording, making it legal to record as long as at least one party has consented to that recording. Adding an additional layer of protection, Washington, along with eleven other states, follows the two-party consent doctrine—requiring consent of all parties engaged in the conversation.[105]

---

95. Brian Heater, *After pushing back, Amazon hands over Echo data in Arkansas murder case*, TECHCRUNCH (Mar. 7, 2017), https://techcrunch.com/2017/03/07/amazon-echo-murder/ [https://perma.cc/Z5AT-RXNH].

96. *Id.*

97. *Id.*

98. Bohm, *supra* note 66 at 12–13.

99. WASH. REV. CODE § 9.73.030 (2019).

100. *See infra* Part IV.

101. Bohm et al., *supra* note 64, at 13.

102. Electronics Communication Privacy Act, § 18 U.S.C. 2510 (2012).

103. Bohm et al., *supra* note 64, at 13.

104. 18 U.S.C. § 2511 (2012).

105. *Recording Phone Calls and Conversations*, DIGITAL MEDIA LAW PROJECT, http://www.dmlp.org/legal-guide/recording-phone-calls-and-conversations [https://perma.cc/K66B-E6RV].

In 1967, Washington adopted the two-party consent doctrine[106] by amending their statute to include a section stating that it was unlawful for:

> [A]ny individual, partnership, corporation, association, or the state of Washington, its agencies, and political subdivisions to intercept, or record any: (1) Private communication transmitted by telephone, telegraph, radio, or other device between two or more individuals between points within or without the state by any device electronic or otherwise designed to record and/or transmit said communication regardless how such device is powered or actuated, without first obtaining the consent of all the participants in the communication; (2) Private conversation, by any device electronic or otherwise designed to record or transmit such conversation regardless how the device is powered or actuated without first obtaining the consent of all the persons engaged in the conversation.[107]

Violations of the statute result in many different consequences. First, anyone that violates the statute is guilty of a gross misdemeanor.[108] Next, anyone that has had their business, person, or reputation injured because of a person's violation of the statute has a civil cause of action against them and is entitled to actual damages, including mental pain and suffering, liquidated damages, a reasonable attorneys' fee, and other costs of litigation.[109] Finally, any information obtained in violation of the statute is not permissible as evidence in civil or criminal cases.[110]

To determine whether there has been a violation of the statute, Washington courts first consider whether the recorded communications were private.[111] If the conversation is found to be private, the court will consider whether the communications were recorded by a device and

---

106. There are situations under RCW § 9.73.030 where recording is appropriate with only one party's consent. WASH. REV. CODE § 9.73.080 (2019). For example, when the owner of a building records conversations of persons engaging in a criminal act in that building; when a police officer has a reasonable suspicion that a conversation involves unlawful activities associated with controlled substances, the criminal prosecution of a violent offense or unlawful engagement of sexual abuse of a minor; or when a chief law enforcement officer, as part of a criminal investigation, records or intercepts communications where at least one party has consented and probable cause exists regarding the contents of the conversation. While such situations are beyond the scope of this comment, it is worth noting that law enforcement agencies need to have clear rules for when they may and may not access the data of speech-activated devices.

107. Act of 1967, ch. 93, 1967 Wash. Ex. Sess. Laws 1819 (codified as WASH. REV. CODE §§ 9.73.030–9.73.080).

108. WASH. REV. CODE § 9.73.080 (2019).

109 WASH. REV. CODE § 9.73.060.

110. WASH. REV. CODE § 9.73.050.

111. State v. Townsend, 147 Wash. 2d 666, 673, 57 P.3d 255, 259 (2002).

whether the parties consented to the recordings.[112] Thus, there are three questions case law answers: (1) which conversations are private; (2) when conversations are recorded by a device; and (3) what constitutes consent.

A. Which Conversations Are "Private"?

Because RCW 9.73.030 only covers "private" conversations and communications, determining the statute's impact on speech-activated devices requires an understanding of how Washington courts have defined "private" and which communications have been protected as "private" within the act.[113]

While the term "private" is not defined in the act, the Washington State Supreme Court has previously used the dictionary definition: "belonging to one's self . . . secret . . . intended only for the persons involved (a conversation) . . . holding a confidential relationship to something . . . a secret message: a private communication . . . secretly: not open or in public."[114] Furthermore, a communication is private (1) when parties manifest a subjective intention that it be private[115]; and (2) where that expectation is reasonable.[116] This inquiry is fact specific and is conducted on a case-by-case basis.[117]

Washington courts have addressed arguments that developments in technology should require objective, rather than subjective, expectations of privacy.[118] In *State v. Faford*,[119] the State essentially tried to argue that because the technology exists to easily intercept cordless telephone conversations, society does not reasonably expect privacy in those calls.[120] However, the court emphasized that "the mere possibility that intrusion on otherwise private activities is technologically feasible does not strip citizens of their privacy rights."[121] In fact, the court stated that, "the

112. *Id.* at 174–75, 57 P.3d at 259–60.

113. WASH. REV. CODE § 9.73.030.

114. *Townsend*, 147 Wash. 2d at 673, 57 P.3d at 259 (2002) (quoting WEBSTERS THIRD NEW INTERNATIONAL DICTIONARY (1969)).

115. State v. Faford, 128 Wash. 2d 476, 485, 910 P.2d 447, 451 (1996). The subjective intent need not be stated explicitly.

116. State v. Christensen, 153 Wash. 2d 186, 193, 102 P.3d 789, 792 (2004).

117. *See* State v. Clark, 129 Wash 2d 211, 227, 916 P.2d 384, 397 (1996).

118. *Faford*, 128 Wash. 2d at 484, 910 P.2d at 451.

119. 128 Wash. 2d 476, 910 P.2d 447 (1996).

120. *Id.*

121. *Id.* at 485, 910 P.2d at 451.

sustainability of our broad privacy act depends on its flexibility in the face of a constantly changing technological landscape."[122]

With the goal of protecting individual privacy rights, the court found that new communications technology should not extinguish any traditional expectations of privacy in telephone calls.[123] More recently, the Washington State Supreme Court found that, "as text messaging increasingly becomes a substitute for more traditional forms of immediate communication, text messages should be afforded the same protections from interception that are recognized for telephone conversations."[124] This language again demonstrates the court's commitment to protecting privacy rights in the face of evolving technology.

Turning to the reasonableness requirement, the Washington State Supreme Court has outlined three non-dispositive factors that courts must consider when determining whether there was a reasonable expectation of privacy. These factors include: (1) the duration and subject matter of the communication; (2) the location of the communication and the potential presence of third parties; (3) and the role of the nonconsenting party and his or her relationship to the consenting party.[125] Generally, longer conversations with sensitive subject matter that occur in discrete locations between family or close friends will be considered private.[126]

Regarding the subject matter aspect of the first element, Washington courts have found that "inconsequential, nonincriminating" conversations are generally not protected under the act.[127] For example, in *Kadorian by Peach v. Bellingham Police Department*,[128] the defendant's daughter answered a telephone call from a stranger, told the caller that her father was not home, and then took a message.[129] Because the duration of the conversation was brief, and the contents of the conversation were inconsequential, nonincriminating, and made to a stranger, the court held that the individuals did not maintain a reasonable expectation of privacy.[130]

---

122. *Id.* at 485–86, 910 P.2d at 451.

123. *See id.*

124. State v. Roden, 179 Wash. 2d 893, 902, 321 P.3d 1183, 1187 (2014).

125. State v. Clark, 129 Wash. 2d 211, 225–26, 916 P.2d 384, 392–93. (1996).

126. *See generally* section III.A.

127. State v. Faford, 128 Wash. 2d 476, 484, 910 P.2d 447, 451 (1996).

128. Kadoranian by Peach v. Bellingham Police Department, 119 Wash. 2d 178, 829 P.2d 1061 (1992).

129. *See id*. at 182, 829 P.2d at 1063.

130. *Id.* at 187, 829 P.2d at 1066.

Unlike the brief and inconsequential conversation in *Kadorian*, in *State v. Kipp*,[131] the Washington State Supreme Court found that a ten-minute-long conversation suggested that the conversation was private.[132] Because the conversation concerned alleged molestation, a conversation not normally intended for the public, the court found that both the duration and subject matter of the conversation demonstrated the defendant's reasonable expectation of privacy.[133]

For the second factor, the court considers both the potential presence of third parties and the location of the communication. The Washington State Supreme Court has held that, generally, the presence of a third party during the conversation means that the matter is not private.[134] Regarding location, Washington courts have found that a private home is normally afforded maximum privacy protection.[135] For example, in *Kipp*, where the conversation took place in the kitchen of a private residence with no third parties present, the court found that the defendant's expectation of privacy was reasonable.[136]

The third factor considers the role of the nonconsenting party and his or her relationship to the consenting party.[137] The Washington State Supreme Court has found that the nonconsenting party's willingness to provide the information to a stranger is evidence that a communication is not private—for example, in *Kadorian*, where a daughter gave information a stranger on the phone.[138] Alternatively, in *Kipp*, because the conversation was between family, the defendant and his brother in law, rather than with a stranger, it provided further evidence of the defendant's

131. 179 Wash. 2d 718, 317 P.3d 1029 (2014).

132. *Id.* at 730, 317 P.3d at 1034.

133. *Id.*

134. State v. Clark, 129 Wash. 2d 211, 226, 916 P.2d 384, 392 (1996); *see also* State v. Flora, 68 Wash. App. 802, 808, 845 P.2d 1355, 1358 (1992) (finding when communications were recorded on a public road in the presence of a third party and within sight and hearing of passersby, there was no reasonable expectation of privacy); State v. Slemmer, 48 Wash. App. 48, 52, 738 P.2d 281, 284 (1987) (finding where an individual attended meetings with multiple other individuals who could easily reveal the conversations to others and those conversations were being recorded in minutes available to the public, the individual did not have a reasonable expectation of privacy).

135. State v. Hastings, 119 Wash. 2d 229, 242, 830 P.2d 658, 665 (1992) (finding where an individual engaged in business transactions with the public in his private home, the individual had no reasonable expectation of privacy). While *Hastings* focused on Fourth Amendment violations, Washington courts have utilized this reasoning for purposes of RCW § 9.73.030 and the two-party consent doctrine.

136. *Kipp*, 179 Wash. 2d at 730, 317 P.3d at 1034.

137. *Clark*, 129 Wash. 2d at 226, 916 P.2d at 393.

138. Kadoranian by Peach v. Bellingham Police Dep't, 119 Wash. 2d 178, 190, 829 P.2d 1061, 1068 (1992).

reasonable expectation of privacy.[139] If a Washington court finds that there was a reasonable expectation of privacy based on these factors, it will then consider if the communication was recorded by a device.[140]

B. When Are Communications Recorded By a Device?

Washington courts have considered whether a recording must be intentional for a communication to be "recorded by a device" and what constitutes a "device." In *State v. Smith*,[141] the Washington State Supreme Court found that both intentional and inadvertent recordings fall within the purview of the Privacy Act.[142] In *Smith*, the defendant's cell phone voicemail accidentally recorded a conversation between the defendant and his wife.[143] Although the recording was accidental, the court found that no specific mental state is required for recording, reasoning that nothing in the plain language of the statute implied a specific mental state.[144] The Court also stated that the statute strives to safeguard private conversations that are recorded in any way, even if those conversations exposed unlawful matters.[145]

When determining what constitutes a "device" for the purposes of the Act, Washington courts have found that computers, among other things, qualify. In *State v. Townsend*,[146] where messages were recorded onto a computer, the state attempted to argue that the communications were not recorded because "'[r]ecording" is simply an inherent part of the use of a computer" and that "prior 'cases all involved use of a device different than the device used to perform the communication itself.'"[147] The court quickly rejected both of these arguments, stating that the communications were recorded onto the computer and that the computer was a device within the parameters of the statute.[148]

---

139. *Kipp*, 179 Wash. 2d at 730, 317 P.3d at 1034.

140. WASH. REV. CODE § 9.73.030 (2019).

141. State v. Smith, 189 Wash. 2d 655, 405 P.3d 997 (2017).

142. *Id.* at 663, 405 P.3d at 1001.

143. *Id.* at 658, 405 P.3d at 999.

144. *Id.* at 662, 405 P.3d at 1001.

145. *Id.*

146. State v. Townsend, 147 Wash. 2d 666, 57 P.3d 255 (2002).

147. *Id.* at 674, 57 P.3d at 259 (quoting Respondent's Brief at 7–8).

148. *Id.*

C. What Constitutes Consent?

Even when a private conversation is recorded by a device, there is no violation of the statute if all parties have consented to that recording. In 1977, the Washington State Legislature amended the statute to explain when consent has been obtained.[149] The language states that:

> Where consent by all parties is needed pursuant to this chapter, consent shall be considered obtained whenever one party has announced to all other parties engaged in the communication or conversation, in any reasonably effective manner, that such communication or conversation is about to be recorded or transmitted: PROVIDED, That if the conversation is to be recorded that said announcement shall also be recorded.[150]

Essentially, a party has consented to a recording when another party has announced, in an effective manner, that the conversation will be recorded and that announcement is recorded.[151] The Washington State Supreme Court has found that consent can be obtained both clearly[152] and implicitly.[153] For example, when there was a recorded message as well as a posted sign alerting an inmate and her grandmother that their conversation would be recorded, the court found that consent had been clearly obtained.[154]

Alternatively, in *State v. Townsend*, the court found that implicit consent might exist if an individual engages in conversations with the knowledge that a "message recording device" is present.[155] In *Townsend,* there were two types of messages at issue: e-mail messages and ICQ messages, a program that allowed users to communicate on the Internet in real-time.[156] The court reasoned that, because the defendant was an e-mail user, he had to understand that computers were "message recording devices," and that his e-mail messages would be recorded onto the recipient's device.[157] Thus, while the *Townsend* Court acknowledged that

---

149. Act of 1977, ch. 363, 1977 Wash. Ex. Sess. Laws 1674 (codified as Wash. Rev. Code § 9.73.030 (2018)).

150. WASH. REV. CODE § 9.73.030(3) (2019).

151. *Id.*

152. State v. Modica, 136 Wash. App. 434, 449, 149 P.3d 446, 454 (2006), *aff'd*, 164 Wash. 2d 83, 186 P.3d 1062 (2008).

153. State v. Roden, 169 Wash. App. 59, 68, 279 P.3d 461, 466 (2012), *rev'd*, 179 Wash. 2d 893, 321 P.3d 1183 (2014); *Townsend*, 147 Wash. 2d at 676, 57 P.3d at 260.

154. *See Modica*, 136 Wash. App. at 449, 149 P.3d at 454 (2006).

155. *Townsend*, 147 Wash. 2d at 678, 57 P.3d at 260.

156. *Id.*

157. *Id.*

the defendant did have a reasonable expectation of privacy regarding the contents of the e-mail messages, there was no violation of the statute because he had implicitly consented.[158]

Whether the defendant had impliedly consented to recordings of messages sent on ICQ was not as readily apparent.[159] Notably, the defendant's ICQ contained a privacy policy that specifically warned users that "[s]ome versions of the software allow any party to an ICQ session to record the content of the session."[160] Based on the court's presumption that the defendant was familiar with the policy and the defendant's general understanding of the technology, the *Townsend* Court found that the defendant had also implicitly consented to recording the ICQ messages.[161]

Alternatively, in a case contemplating the privacy of text messages, the Washington State Supreme Court found that using iMessage did not necessarily manifest implicit consent.[162] In *State v. Roden*,[163] the Washington Court of Appeals employed similar reasoning to *Townsend*, finding that iPhones are "message recording devices" and that the defendant should have known that the iPhone would record and store his messages.[164] However, the Washington State Supreme Court reversed on other grounds and stated that they would not reach the issue of implicit consent.[165]

Because the *Roden* Court did not reach the issue, it is unclear whether the Washington State Supreme Court would conclude that an iPhone or other device is a "message recording device" providing implicit consent. Still, if an individual engages in private conversation with the knowledge that a "message recording device" (as designated by the court) is present, it is possible that they have implicitly consented.[166]

---

158. *Id.*

159. *Id.*

160. *Id.* at 677, 57 P.3d at 261 (quoting Clerk's Papers at 139, State v. Townsend, 147 Wash. 2d 666, 57 P.3d 255 (2002) (No. 193047) [hereinafter *Townsend* Clerk's Papers]).

161. *Id.* "The ICQ privacy policy also warned users that they risk '[u]nauthorized exposure of information and material you listed or sent, on or through the ICQ system, to other users, the general public or any other specific entities for which the information and material was not intended by you.'" *Id.* (quoting *Townsend* Clerk's Papers, *supra* note 158, at 139).

162. State v. Roden, 179 Wash. 2d 893, 900, 321 P.3d 1183, 1186–87 (2014).

163. State v. Roden, 169 Wash. App. 59, 279 P.3d 461 (2012), *rev'd*, 179 Wash. 2d 893, 321 P.3d 1183 (2014).

164. *Id.* at 67, 279 P.3d at 466.

165. *Roden*, 179 Wash. 2d at 904, 321 P.3d at 1188 (2014) (finding that the act had not been violated because *Roden* turned on whether the text messages had been "intercepted" while *Townsend* turned on whether the messages had been "recorded").

166. *Townsend*, 147 Wash. 2d at 675, 57 P.3d at 260.

IV. ALEXA AS APPLIED TO WASHINGTON'S TWO-PARTY CONSENT LAW

To recap, when determining whether a violation has occurred, a Washington court will look at: (1) whether the conversation was private; (2) whether the conversation was recorded by a device; and (3) whether there was implicit or explicit consent.[167] One can surely imagine a situation where a private conversation is recorded by an Echo. For example, because Echos are usually found in homes, it is likely that they will overhear private conversations between family members or close friends.

The requirement that the conversation be recorded by a device is also easily met. Although scholars have argued that information recorded by virtual assistant devices are more akin to data from a computer rather than wiretapping,[168] Washington courts have already held that computers are recording devices within the statute because communications are recorded on to them.[169] Similarly, because Amazon is clear about the fact that the Echo records communications,[170] the Echo is likely a recording device for the purposes of the statute. Whether a recording is inadvertent is irrelevant because accidental recordings fall within the purview of the act.[171] Thus, while the first two questions are readily answered, whether an individual has consented is a more difficult question.

A. Explicit Consent

A filing in an ongoing lawsuit[172] in the Western District of Washington suggests that non-registered users do not explicitly consent to being recorded when they use the device.[173]

---

167. *See supra* Part III.

168. Lenore E. Benessere & Robert D. Lang, *Virtual Assistants in the Workplace: Real, Not Virtual Pitfalls and Privacy Concerns*, 21 No. 12 J. INTERNET L. 1, 20 (2018).

169. *See* State v. Townsend, 147 Wash. 2d at 676, 57 P.3d at 260.

170. *Alexa and Alexa Device FAQs*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=201602230 [https://perma.cc/P75S-7BL6].

171. *See supra* Part III.

172. This complaint, filed in the Western District of Washington, claims that Amazon's Alexa violated Washington and other states two-party consent laws by recording children without their consent. This argument is pending in ongoing litigation. *See generally* Complaint, C.O. v. Amazon, Inc., No.: 2:19-cv-910 (W.D. Wash. June. 6, 2019), https://static1.squarespace.com/static/5a6a87cee45a7cb3647a8ee5/t/5d004e1aa0d35c00016f30e9/1560301082577/2019.06.11+DN+1+Complaint.pdf [https://perma.cc/KS8X-HWJW].

173. Report and Recommendation at 3, B.F. & A.A. v. Amazon, No. C19-910-RAJ-MLP (W.D. Wash. Oct. 21, 2019).

The plaintiffs in that suit, *B.F. & A.A. v. Amazon*,[174] argued that Amazon's Alexa violated Washington's and other states' two-party consent laws by recording children without consent.[175] Amazon filed a motion to compel the claims into arbitration.[176] When determining whether the children agreed to arbitrate the claim through Amazon's Conditions of Use or Alexa's Terms of Service, a magistrate judge stated that, "[i]t is undisputed that because Plaintiffs are not account holders with Amazon, they did not personally enter into any contractual agreement with Amazon before using the Alexa devices at issue." Furthermore, she concluded that binding a non-primary user to the arbitration provisions "would lead to absurd results, as even a casual visitor to a residence could be bound by an agreement without notice."[177]

While *B.F & A.A. v. Amazon* centers on an arbitration provision, it seems quite reasonable to imply that most guests to an Echo-owner's home have not agreed to Amazon's Conditions of Use or Alexa's Terms of Use and thus have not clearly consented to being recorded. Furthermore, Amazon does not take any other steps to gain clear consent of non-registered users such as playing a message informing the individual that they are being recorded or cease recording when they hear a user that they do not recognize.

Amazon could argue that an Echo-owner agrees to gain the consent of any guests in their home when they agree to, "accept responsibility for all activities that occur under [their] account of password," under Amazon's Conditions of Use.[178] However, Washington's privacy law requires the individual or corporation that records the private conversation to obtain consent.[179] And in this case, plaintiffs likely have strong arguments that Amazon rather than the device-owner is the one required to gain consent. After all, Amazon is the entity recording, storing, and analyzing those conversations.

B. Implicit Consent

A more plausible argument for consent is that a guest in an Echo-owner's home implicitly consents to being recorded. In *Townsend*, the

174. No. C19-910-RAJ-MLP (W.D. Wash. Oct. 21, 2019).

175. *Id.*

176. *Id.*

177. *Id.*

178. *Amazon Conditions of Use,* AMAZON, https://www.amazon.com/gp/help/customer/display.html?ie=UTF8&%2AVersion%2A=1&%2Aentries%2A=0&nodeId=508088 [https://perma.cc/NNK6-P2P9].

179. WASH. REV. CODE § 9.73.030 (2019).

Court looked at the nonconsenting party's familiarity with the technology and his understanding that a computer was a "message recording device" to find that the defendant had implicitly consented to the recording of his e-mail messages.[180] If an individual asked Alexa a question, a court might employ similar reasoning to find implicit consent: the non-device-owner is familiar with the Alexa technology; understands that to execute the command, the device will record the conversation; and sees the blue light indicating recording.

But there are certainly situations where a guest does not implicitly consent to being recorded. For example, a guest walks into an Echo-owner's home where the device is actively playing music but also recording. They have no knowledge that the device is even in the room, and they discuss private matters that are recorded by the device. In this scenario, a guest likely has not consented to being recorded, and a violation of the two-party consent doctrine has occurred.

A court might also reason that virtual assistant devices are becoming increasingly popular and thus an individual has implicitly consented to the recording if they even see an Alexa device in the room. However, the devices have not yet become so prevalent and customary in homes and Washington courts should hesitate before making such assumptions. Even Echo-owners are not always familiar with the recording aspect of Alexa technology, evidenced by users asking, "Alexa, is anyone else listening to us?"[181] Presuming familiarity with the Alexa technology or its privacy policies would be at odds with the goal of the statute—protecting privacy rights in the face of evolving technology.

Washington courts have addressed similar arguments in the past. In *State v. Faford*, the State tried to argue that because the technology exists to easily intercept cordless telephone conversations, society implicitly consents to those interceptions.[182] However, the Court emphasized that "the mere possibility that intrusion on otherwise private activities is technologically feasible does not strip citizens of their privacy rights."[183] Similarly, when faced with the potential ubiquity of virtual assistant devices like Amazon's Alexa, Washington courts should strive to maintain citizens' privacy rights rather than assuming implicit consent.

With Amazon transcribing voice clips and inadvertently sending out recordings, the risk of a disclosure of private conversations certainly exists. One can imagine a situation where sensitive information falls into the

180. *Townsend*, 147 Wash. 2d at 676, 57 P.3d at 260.

181. *Supra* Part II.

182. State v. Faford, 128 Wash. 2d 476, 489, 910 P.2d 447, 453 (1996).

183. *Id.* at 485, 910 P.2d at 451.

wrong hands and exposes an individual to harm. As virtual assistants become increasingly popular, it is vital that the Washington State Legislature is proactive in addressing the increasing risks that they present.

V. POTENTIAL SOLUTIONS TO THE CONFLICT BETWEEN VIRTUAL ASSISTANT DEVICES AND TWO-PARTY CONSENT LAWS

While there are proposed solutions to the tension between speech-activated devices and two-party consent laws, there are no solutions that fully address potential risks, place responsibility on the proper party, or provide an action for relief against manufacturers of devices.

A. Shortcomings of Proposed Solutions

Some scholars argue that a pragmatic solution would be to place the responsibility of getting consent on the owner of a device rather than Amazon because of the difficulties Amazon would encounter in attempting to obtain consent from third parties.[184] For example, even if Amazon were to reference two-party consent laws in their policies, a guest of an Echo-owner would not have the chance to see the terms or to agree to them. Moreover, if Alexa were to state a warning that conversations were being recorded when it was initially turned on, it would prove ineffective for those guests that arrived after the device had played the message.

Regardless of such difficulties, Washington law requires the entity that records the private conversation to gain consent, and Amazon is the entity recording, storing, and analyzing those conversations.[185] Furthermore, in many of the situations reported, inadvertent recordings occurred because of a technological mistake by the device, not because of the owner's use of it.[186] Thus, there is a strong argument that the manufacturer of the device should be required to get consent rather than the owner. Most importantly, unlike many Echo users, Amazon has the resources to remedy individuals for the harm that they cause.

Another solution proposes that service providers distinguish between personally identifiably information pertaining to the Echo-owner and individuals other than the owner, and permanently delete any personally identifiable information that is not the owner's.[187] Because Alexa is capable of differentiating between voices, an Alexa device could

184. Davidian, *supra* note 16, at 60.

185. *See supra* Part IV.

186. *See supra* section II.A.

187. Bohm et al., *supra* note 64, at 3.

presumably listen for consenting users and stop listening when a nonconsenting party is speaking or delete their recordings, similar to how the device constantly deletes voice recordings used to detect the wake word.[188] Like Apple, Amazon could also randomize their data, rather than connecting recordings to individual users.[189] However, because there is no public evidence that Amazon is interested in taking such actions, the risk of harm remains.

A third solution would be to mirror the Anti-Eavesdropping Act that the California State Assembly's privacy committee recently advanced.[190] The Anti-Eavesdropping Act seeks to prohibit recordings or transcripts by the manufacturer of a virtual assistant device.[191] If the recording contains personal information or is not deidentified, the Act states that it should not be used for advertising purposes, shared or sold to a third party, or retained at any location unless the user provides consent.[192] It requires that all actions for relief are brought by the Attorney General.[193]

While the Anti-Eavesdropping Act offers protection against owners of virtual assistant devices, it does not allow individuals whose privacy rights are violated to raise a claim themselves. Consequently, the Washington State Legislature should both create an Act that mirrors the Anti-Eavesdropping Act and carve out a cause of action against virtual assistant device developers and manufacturers for individuals.

B. The Washington State Legislature Should Clarify that the Onus Falls on the Manufacturer for Private Recordings

The Washington State Legislature has clearly demonstrated the value it places on protecting individual's privacy rights by its enactment of the two-party consent law. Moreover, Washington courts have recognized the importance of maintaining these values in the face of a rapidly evolving technology landscape.[194] Accordingly, to curb negative consequences resulting from any ambiguities in the statute, the Washington State Legislature should carve out clear penalties against the manufacturers of virtual assistant devices for when they release surreptitious recordings.

188. *See supra* Part I.

189. *See supra* Part I.

190. Assemb. Bill 1395, 2019 Leg., 2019–2020 Sess. (Cal. 2019).

191. *Id.*

192. *Id.*

193. *Id.*

194. State v. Faford, 128 Wash. 2d 476, 489, 910 P.2d 447, 453 (1996).

Currently, under RCW 9.73.060, a civil cause of action exists for those individuals harmed by unlawful recordings.[195] The language reads as such:

> Any person who, directly or by means of a detective agency or any other agent, violates the provisions of this chapter shall be subject to legal action for damages, to be brought by any other person claiming that a violation of this statute has injured his or her business, his or her person, or his or her reputation. A person so injured shall be entitled to actual damages, including mental pain and suffering endured by him or her on account of violation of the provisions of this chapter, or liquidated damages computed at the rate of one hundred dollars a day for each day of violation, not to exceed one thousand dollars, and a reasonable attorney's fee and other costs of litigation.[196]

At first blush, such language seems to cover a situation where a company inadvertently sends out a potentially harmful recording. However, the Washington State Legislature should consider carving out an explicit cause of action against the manufacturer of the device. Accordingly, the amended statute should read:

> Any person who, directly or by means of a detective agency or any other agent, violates the provisions of this chapter shall be subject to legal action for damages, to be brought by any other person claiming that a violation of this statute has injured his or her business, his or her person, or his or her reputation. **[Any manufacturer or developer, of any device electronic or otherwise designed to record or transmit, that violates the provisions of this chapter shall be subject to legal action for damages, to be brought by any other person claiming that a violation of this statute has injured his or her business, his or her person, or his or her reputation.]** A person so injured shall be entitled to actual damages, including mental pain and suffering endured by him or her on account of violation of the provisions of this chapter, or liquidated damages computed at the rate of one hundred dollars a day for each day of violation, not to exceed one thousand dollars, and a reasonable attorney's fee and other costs of litigation.

With the addition of this language, the Washington State Legislature could delineate clear lines between a cause of action against the owner of a virtual assistant device and a cause of action against the manufacturers and developers of a virtual assistant device. While there may be a situation where a device-owner is at fault, many disclosures are a result of

195. WASH. REV. CODE § 9.73.060.

196. *Id.*

Amazon's actions and this language would make routes against the owner and the manufacturer available to a harmed person.

Such an amendment could result in other benefits as well. For example, it would encourage large companies like Amazon to work toward improving their technologies and minimizing situations where Alexa is recording private conversations. Also, because consumers like to be in control of their information, providing a remedy for the lack of consent would be beneficial to Amazon's business.[197]

This broad language would be effective in the context of two-party consent laws because it considers rapidly changing technologies. As the Washington State Supreme Court has previously noted, "the sustainability of our broad privacy act depends on its flexibility in the face of a constantly changing technological landscape."[198] By mirroring the language in RCW 9.73.030, this proposed language leaves room for technologies other than virtual assistant devices that might emerge and give rise to similar tensions. Thus, by amending the statute to include this language, the Washington State Legislature can ensure that they are affording individuals adequate protection when it comes to virtual assistant devices and that companies are held accountable for recording private conversations in violation of the two-party consent doctrine.

CONCLUSION

Amazon's Alexa is an incredible piece of technology. The virtual assistant can learn personal preferences, increase efficiencies, and even tell jokes. It can assist people with disabilities, making their lives easier. Companies should be encouraged to create new technologies and better people's lives. However, such improvements should not come at the cost of individuals' privacy rights.

An Alexa device is recording whenever it is activated, regardless of whether the device was turned on by a wake word or inadvertently. All of those recordings are sent to Amazon's cloud, where they remain until an owner asks for them to be deleted. Although Washington's two-party consent laws require that all individuals subject to a recording provide consent, guests to an Alexa-owner's house are unlikely to do so. Still, those recordings will end up in Amazon's cloud and potentially in a stranger's home.

---

197. MATT CAGLE, ET AL., PRIVACY & FREE SPEECH: IT'S GOOD FOR BUSINESS 16–18 (ACLU of Cal., 3d ed. 2016), https://www.itsgoodfor.biz/sites/default/files/Privacy%20and%20Free%20Speech%20Primer%20-%20Volume%203.pdf [https://perma.cc/CRZ9-ZPDF].

198. *Faford*, 128 Wash. 2d at 485–86, 910 P.2d at 451.

The Washington State Legislature should curb these risks by amending the privacy statute to include a cause of action against manufacturers that violate the statute and creating a statute that mirrors the Anti-Eavesdropping Act. With this cause of action, any ambiguities surrounding liability will be dispensed and the proper parties will be held accountable. Moreover, large companies will be further incentivized to improve their products and customer experiences.

As new technologies arise and virtual assistant devices become more and more prevalent, it is important for the Washington State Legislature to address risks associated with the devices proactively. By creating both a cause of action against manufacturers and an Act that mirrors the Anti-Eavesdropping Act, the Washington State Legislature can continue to be at the forefront of protecting privacy rights.