Mercer Law Review

Volume 71
Number 2 *Articles Edition*

Article 7

3-2020

# An Uneasy Love Triangle Between Alexa, Your Personal Life, and Data Security: Exploring Privacy in the Digital New Age

Marissa Merrill

# An Uneasy Love Triangle Between Alexa, Your Personal Life, and Data Security: Exploring Privacy in the Digital New Age*

## I. INTRODUCTION

Would you willingly welcome a stranger into your home to listen and record your private conversations? You might have already done so if you own a voice-controlled, personal assistant device like Amazon's Alexa products. These devices listen to your conversations and record your interactions awaiting a command, sending personal data through the cloud to Amazon employees to translate the information into an action. So how private is your personal data if it's being shared through these devices?

For years people have dreamed about the technology of the future. But these technological advances open the door to new, different problems. Voice-controlled, personal assistant devices have become the norm, earning its space on our kitchen counters, living room tables, bedroom nightstands, and inside our hand-held devices. With the sound of your voice, this technology is alert and ready to take action. Yet, the problem lies within that technology and it exists because of the ease. While these devices are listening for the user's command, they also record interactions and personal information to personalize or improve each user's experience. However, there is one lingering concern about the interactions with such voice-controlled, personal assistant devices: how private is the personal data it consumes?

This Article explores privacy concerns in a world of technological advancements and ease. While examining the recent privacy and legal issues with these devices, this Article will analyze the current state of

*To my family and close friends, I am immensely grateful for your unwavering encouragement and guidance. I would also like to thank Professor Anne Johnson for her helpful advice and support throughout the writing process.

privacy laws and compare it to other regions for a conclusion on how to best protect your data.

## II. THE DEVICES: THE DIGITAL NEW AGE

### *A. Voice-Controlled, Personal Assistant Devices*

Voice technology is the future and many new devices have built-in personal assistants activated by voice commands.[1] In 2018, PricewaterhouseCoopers (PwC) conducted a survey about consumers' familiarity with voice-controlled devices.[2] Of the respondents, 72% had used a product equipped with voice technology.[3] More specifically, 57% had used voice-assistant programs on a smartphone, 29% on a laptop, and 27% on a speaker.[4] Younger consumers, ages eighteen to twenty-four years old, are driving this new trend and encouraging the usage of such devices.[5] Although these voice-controlled devices are mobile, "three out of every four consumers (74%) are using their mobile voice assistants at home."[6] Consumers reported using voice technology to assist them in multiple everyday tasks.[7] These tasks include asking a simple question, checking the weather, asking for the news report, sending texts or emails, and purchasing online products.[8] A large majority of people found the new technology to be "the smarter, faster, and easier way to perform everyday activities."[9]

In addition to welcoming voice-assistant devices into their homes, the survey reported that 44% of people used their device to control another product in their home.[10] As a result, this technology is potentially linked to bank accounts, security systems, televisions, personalized calendars, contact lists, and personal conversations.[11] The survey also reported that 9% of respondents had never used a voice assistant and had no plan to use one in the future.[12] Why? Because of privacy

1. *PwC Consumer Intelligence Series Voice Assistants Survey*, PWC, 1–12, 2 (2018), https://www.pwc.com/us/en/advisory-services/publications/consumer-intelligence-series/pwc-voice-assistants.pdf.
2. *Id.*
3. *Id.* at 3.
4. *Id.*
5. *Id.*
6. *Id.*
7. *Id.*
8. *Id.* at 4.
9. *Id.* at 5.
10. *Id.* at 7.
11. *Id.*
12. *Id.* at 8.

concerns; specifically, these respondents were uneasy about the device constantly listening and the security of their personal data.[13] Despite these concerns, "[t]he average consumer is using their voice assistant more than they were before, and will use it even more in the future."[14]

As the technology of voice assistants progresses, companies must balance the "fine line between being 'cool' or 'helpful' and being 'creepy[,]' [because] [t]he key is to use personal consumer data in a secure and transparent way to create personalized experiences that the consumer wants and has asked for."[15]

### *B. Popular Devices with Voice-Controlled Assistants*

Voice-controlled, personal assistant devices come in all shapes and sizes and are marketed by many popular companies. This new technology is fascinating and was quickly picked up by powerhouse developers. Many major companies have their own variation of a digital assistant: Amazon's Alexa, Apple's Siri, Microsoft's Cortana, and the Google Assistant.[16] This Article focuses specifically on the voice technology and experience with Alexa-enabled Amazon products to address a widespread privacy concern with all similar devices.

### *C. Amazon's Alexa-Enabled Devices*

Amazon markets its Alexa devices by stating "[w]ith Alexa, you can build natural voice experiences that offer customers a more intuitive way to interact with the technology they use everyday."[17] The company also poses extensive privacy protections, with "transparency and control over your Alexa experience."[18]

Amazon offers three different sized speakers called Echos. Each device is designed with four buttons on its face: two volume buttons, an action button, and a microphone-off button.[19] The device lights up with

---

13. *Id.*

14. *Id.* at 9.

15. *Id.* at 10.

16. Eric Boughman, Sara Beth A.R. Kohut, David Sella-Villa, Michael V. Silvestro, *"Alexa, Do You Have Rights?": Legal Issues Posed by Voice-Controlled Devices and the Data They Create*, American Bar Association (July 20, 2017), https://www.americanbar.org/groups/business_law/publications/blt/2017/07/05_boughman/?q=&fq=(id%3A%5C%2Fcontent%2Faba-cms-dotorg%2Fen%2Fgroups%2Fbusiness_law%2F*)&wt=json&start=0.

17. *What is Alexa?*, AMAZON, https://developer.amazon.com/en-US/alexa (last visited Nov. 30, 2019).

18. *Alexa Privacy*, AMAZON, https://www.amazon.com/b/?node=19149155011 (last visited Nov. 30, 2019).

19. *Id.* at 18.

a blue ring to signal that Alexa is recording the interaction and sending requests to the cloud.[20] Amazon's Alexa is suited with learning technology to help improve the users' experience with the device and provide assistance in a personalized way because "Alexa is designed to get smarter every day."[21] While these features use personal data to improve the experience, the company allows users to turn off such learning features.[22] Consequently, the user who chooses to do so will have inhibited the learning technology and stunted personalized improvements for their device.

Amazon's Alexa is popular because of its extensive capabilities. The company quotes that the devices have "hundreds of thousands of supported commands."[23] A list of supported commands includes the ability to set calendar appointments, connect to Bluetooth, communicate through calls and messages, purchase online products, play games, tell jokes, read weather reports, and much more.[24] While these features assist the user with everyday activities, the information shared between the two is sent into the cloud to be processed. As you will see later in this Article, Amazon creates a file of information from each device, which serves as a glimpse into your private life pieced together from your communications with "Alexa."

As of January 2019, over 100 million Alexa-enabled devices were sold worldwide.[25] Although people welcome these devices into their homes, a 2018 survey noted that 28% of people are concerned about their data privacy.[26] More specifically, 38% were concerned with the Amazon product listening to their private conversations.[27] A different online survey with 5,716 responses reported that 56% of respondents found

---

20. *Id.*

21. *Privacy Settings*, AMAZON, https://www.amazon.com/b/?node=19149164011 (last visited Nov. 30, 2019).

22. *Id.*

23. *Use Alexa: Things to Ask Alexa*, AMAZON, https://www.amazon.com/b/ref=aeg_lp_tycaa_d_text/ref=s9_acss_bw_cg_aegflp_md1_w?node=17934693011&pf_rd_m=ATVPDKIKX0DER&pf_rd_s=merchandised-search-6&pf_rd_r=1FKR59ZPAX1VBGX9NB1H&pf_rd_t=101&pf_rd_p=02147624-e148-4901-b449-773097cfa62e&pf_rd_i=17934672011 (last visited Nov. 30, 2019).

24. *Id.*

25. Eric Johnson, *Think about privacy the next time you ask Alexa about the weather*, THE NEXT WEB (March 16, 2019, 13:30 UTC), https://thenextweb.com/podium/2019/03/16/think-about-privacy-the-next-time-you-ask-alexa-the-weather/.

26. PWC, *supra* note 1, at 8.

27. *Id.*

Alexa's listening and recording habits to be "creepy."[28] Throughout the following sections, this Article analyzes these consumer concerns and recorded instances of a breach in data privacy.

Before addressing the issues with these devices and personal privacy, it is important to highlight Amazon's privacy policy. The company provides that "[y]ou can view, hear, and delete your voice recordings at Alexa Privacy Settings or in the Alexa app at any time. To delete by voice, you can also say, 'Alexa, delete what I just said' or 'Alexa, delete everything I said today.'"[29] The privacy settings allow for users to enable a feature called "auto-delete."[30] Yet enabling these protective features, such as deleting your recorded information, "may degrade your Alexa experience."[31]

Amazon also puts users on notice that their recordings may be reviewed, stating that "[a]n extremely small fraction of voice recordings are manually reviewed to improve Amazon services and develop new features."[32]

## III. THE PROBLEM: DATA BREACHES AND PRIVACY CONCERNS

Although the PwC survey from 2018 reported user satisfaction with voice-controlled, personal–assistants, respondents also reported serious privacy concerns.[33] While 50% of consumers had used their voice assistant device to make an online purchase, which created a direct link to their credit card or bank account and the device, another 45% stated they did not feel comfortable paying through the device.[34] One respondent was uneasy about the ability of the device to process payments through her account, stating "[t]his reminds me of when my daughter racked up almost $1,500 playing a mobile game . . . Can it get to a point where the device can confirm it's me who's talking and not my 11-year-old who's going rogue?"[35]

Voice-assistant devices are equipped with learning technology. Two key components of this technology are listening and recording its

28. Mozilla *privacy not included, *Amazon Echo & Dot*, https://foundation.mozilla.org/en/privacynotincluded/products/amazon-echo-dot/ (last visited Nov. 30, 2019).

29. *Alexa Privacy*, *supra* note 18.

30. *Privacy Settings*, *supra* note 21.

31. *Common Questions*, AMAZON, https://www.amazon.com/b/?node=19149165011 (last visited Nov. 30, 2019).

32. *Privacy Settings*, *supra* note 21.

33. PWC, *supra* note 1, at 8.

34. *Id.* at 6.

35. *Id.*

interactions with consumers to create a more personalized experience to better assist each user.[36] Yet, because of these critical features, many consumers' concerns about a security breach of their personal data have been brought to life through interesting scenarios since the technology's creation.[37]

In mid-2018, Amazon's Alexa misinterpreted a private conversation between a woman and her husband to be a user command to send a voice message to an outside party.[38] The Alexa-enabled product recorded the conversation and sent the message to one of the couple's contacts.[39] The Amazon company explained the scenario by detailing that Alexa had asked confirmation questions before completing the command.[40] However, the couple from the incident explained that they were not speaking directly to the Amazon product, and instead, were having a private conversation from which the product heard and reacted to words of confirmation picked out of the conversation.[41]

In March 2018, Amazon again came under criticism for its Alexa-enabled products due to instances of unprompted "creepy" laughing from the device.[42] The company responded by disabling the programmed command, "Alexa, laugh," which initiated the laughter, to "Alexa, can you laugh?"[43] Amazon classified these incidents of unprompted actions as "false positives."[44] Although the laughing incidents were not necessarily an invasion of privacy, it signaled to consumers the ability of Alexa to have a mind of its own and to do things without the user's initiation.[45] This example of the learning technology acting on its own is the crux of consumers' security concerns with trusting such a device with their privacy.[46]

---

36. *See* Johnson, *supra* note 25.

37. *Id.*

38. Tom Warren, *Amazon Explains how Alexa Recorded a Private Conversation and Sent it to Another User*, THE VERGE (May 24, 2018, 5:56 PM), https://www.theverge.com/2018/5/24/17391898/amazon-alexa-private-conversation-recording-explanation.

39. *Id.*

40. *Id.*

41. *Id.*

42. Shannon Liao, *Amazon has a Fix for Alexa's Creepy Laughs*, THE VERGE (Mar. 7, 2018, 1:44 PM), https://www.theverge.com/circuitbreaker/2018/3/7/17092334/amazon-alexa-devices-strange-laughter.

43. *Id.*

44. *Id.*

45. *Id.*

46. *Id.*

## IV. THE EXTENT OF AMAZON'S COLLECTED DATA

### *A. Personal Recorded Data Files in the Wrong Hands*

Concerned with data privacy, one Amazon consumer requested his personal file from the company in accordance with European Privacy laws in August 2018.[47] In response, the company sent a 100 megabyte zip file supposedly containing information in connection with his Amazon account.[48] However, this user received approximately 1,700 waveform audio files of recorded interactions with "Alexa" and a pdf document of conversation transcripts, despite him not having an Alexa-enabled device and never using the voice-controlled, personal assistant feature.[49] This information was the personal data of another user, who had no connection to the request for personal files.[50] The company was not aware of its inadvertent personal data breach until the requester notified customer service of the mix-up.[51]

In an effort to analyze the extent of the breach, an investigative company reviewed the files to understand just how much "Alexa" knows about a user's personal life.[52] The recordings covered an entire month and clearly depicted both a male and female voice, in different locations.[53] The investigative company even noted that "Alexa was obviously able to hear our 'subject' in the shower . . . ."[54] Using the files, the company was able to discover details about the subject's personal life, including his location from weather inquires and personal contacts.[55] This information led to the discovery of the subject's social media accounts, and ultimately, a real-life introduction with the subject, who was the victim of the data breach.[56] Amazon responded,

---

47. Holger Bleich, *Alexa, Who Has Access to My Data?: Amazon Reveals Private Voice Data Files*, INVESTIGATIVE ALEXALEAKS, https://www.heise.de/downloads/18/2/5/6/5/3/9/6/ct.0119.016-018_engl.pdf (last visited Nov. 30, 2019).

48. *Id.*

49. *Id.*

50. *Id.*

51. *Id.*

52. *Id.*

53. *Id.*

54. *Id.*

55. *Id.*

56. *Id. See also* Filip Truta, *Amazon Mistakenly Sends Couple's Alexa Recordings to Stranger*, BITDEFENDER BOX, https://www.bitdefender.com/box/blog/iot-news/amazon-mistakenly-sends-couples-alexa-recordings-stranger/ (last visited Nov. 30, 2019); Jenna Kerstein, *Voice-enabled Devices and Data Privacy: Lessons Learned from Amazon*,

calling this privacy disaster an "unfortunate mishap."[57] It further claimed that its devices keep recordings of their user's interactions for its technology to learn from the commands and responses for a more personalized experience with the assistant.[58] Others are wary of this practice, saying such privacy invasions "would never have occurred if Amazon had deleted the voice files in a timely fashion instead of saving them indefinitely in the cloud."[59] However, it is important to note that the company gives the right to its consumers to review and delete their personal recordings from their accounts online at amazon.com/alexaprivacy.[60]

*B. Amazon Listening to Recorded Private Data*

"Millions more are reluctant to invite the devices and their powerful microphones into their homes out of concern that someone might be listening. Sometimes, someone is."[61] Amazon employers are tasked with improving Alexa's understanding of human interactions and the response to specific user commands.[62] In order to effectuate the learning technology, these employees must review recorded data and transcribe it.[63] The employees work nine hour shifts where they review approximately 1,000 audio clips from Alexa users worldwide.[64] One worker recalled an assignment where he reviewed clips for references to Taylor Swift to categorize the reference as the music artist.[65] On occasion, listeners would hear intimate clips, such as a woman singing in the shower.[66] When the employees begin to hear private conversations where the users are talking about people or bank

---

KIRKPATRICKPRICE, https://kirkpatrickprice.com/blog/voice-enabled-devices-and-data-privacy-lessons-learned-from-amazon/ (last visited Nov. 30, 2019).

57. Bleich, *supra* note 47.

58. *Id.*

59. *Id.*

60. *Id.*

61. Matt Day, Giles Turner, and Natalia 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. *See also* Kate O'Flaherty, *Amazon Staff Are Listening To Alexa Conversations–Here's What To Do*, FORBES (April 12, 2019), https://www.forbes.com/sites/kateoflahertyuk/2019/04/12/amazon-staff-are-listening-to-alexa-conversations-heres-what-to-do/#47e5123f71a2.

62. *Id.*

63. *Id.*

64. *Id.*

65. Day et al., *supra* note 61.

66. *Id.*

accounts, the listener is supposed to mark the file as "critical data" and move on to the next file.[67]

An Amazon spokesperson responded to a Bloomberg article by stating that "[a]ll information is treated with high confidentiality and we use multi-factor authentication to restrict access, service encryption and audits of our control environment to protect it."[68] However, the company only puts consumers on notice that "[a]n extremely small fraction" of their recorded data is listened to by Amazon employees and instead the company focuses this notice as efforts to train the learning technology.[69] Similarly, Apple and Google have employees who interpret user requests and assist the technology in their personal assistant devices.[70] As Amazon makes clear in its privacy policy, there are safeguards in place for consumers concerned with others listening to their private conversations.[71] The main safeguard being the visual signal of the blue ring that the device is listening and recording.[72] However, there are instances, as mentioned throughout this Article, of false positives where the device becomes engaged by accident. In Bloomberg's article, with help from two Amazon listener–employees, they reported about 100 recordings each day where the device was accidentally engaged, yet reviewers were still tasked with transcribing the recording.[73]

## V. RELATED LAWS

### *A. Federal Wiretap Act*[74]

The Federal Wiretap Act is codified at 18 U.S.C. §§ 2510–2523 and prohibits the interception or disclosure of wire, oral, or electronic communications.[75] While this Act protects electronic communications, the development of learning technology such as Amazon's Alexa, is centered around its ability to interact and respond to electronic communications. Consumers of these Amazon products are knowingly interacting with the technology, meanwhile real people employed by Amazon are accessing the device's communications. The idea that

67. *Id.*
68. *Id.*
69. *Privacy Settings*, *supra* note 21; Day et al., *supra* note 61.
70. Day et al., *supra* note 61.
71. *Id.*
72. *Id.*
73. *Id.*
74. 18 U.S.C. §§ 2510–2523 (2019).
75. *Id.*

Amazon employees are listening to private recordings and transcribing these communications is seemingly in violation of the spirit of the Federal Wiretap Act. However, the Wiretap Act allows an exception for telephone companies to improve service by listening "for mechanical or service quality control checks."[76] Yet, the drafters of this Act, "never imagined that a telephone company could have a commercial interest in the contents of a phone call."[77] Similarly, the personal assistant technology focuses on learning about its user to create a personalized experience during each interaction, including for a commercial gain.

### *B. Child Online Privacy Protection Act*[78]

The Children's Online Privacy Protection Act (COPPA) prohibits "an operator of a website or online service directed to children, or any operator that has actual knowledge that is collecting personal information from a child, to collect personal information from a child in a manner that violates the regulations . . ."[79] which require notice, parental consent, and maintenance of reasonable procedures to protect the security of the children.[80] This Act was implemented to protect the personal information of children from being disseminated online in order to protect the most vulnerable members of our society.[81] Children must be shielded because they do not understand the implications of using this technology that keeps a record of their personal information.

### *C. Proposed Legislation*

"Currently there are about 7 billion connected devices in the world, according to [Internet of Things] IoT Analytics, an industry research company. It anticipates this number to skyrocket to 21.5 billion devices by 2025."[82] The Internet of Things is a term describing the concept of connectivity between multiple things, including different devices, the

---

76. 18 U.S.C. § 2511(2)(a)(i).

77. Ben Tobin, *Amazon Employees Listen to Customers Through Echo Products, Report Finds*, USA TODAY (April 11, 2019), https://www.usatoday.com/story/tech/2019/04/11/amazon-employees-listening-alexa-customers/3434732002/.

78. 15 U.S.C. §§ 6501–6506 (2019).

79. 15 U.S.C. § 6502(a)(1) (2019).

80. 15 U.S.C. § 6502(b) (2019).

81. *Id.*

82. Jason Tashea, *California imposes new regulations on 'internet of things' devices*, ABA JOURNAL (Dec. 10, 2018), http://www.abajournal.com/news/article/new_california_imposes_regulations_on_the_internet_of_things.

Internet, and people.[83] This concept has grown rapidly with the creation of new devices and the transfer of data between users and their sophisticated products.[84] Naturally, security is a concern with the Internet of Things because of the personal data that flows between the intricate web of connected things.

The Amazon company uses the idea of the Internet of Things to create, to power, and to improve their products and services.[85] The learning technology of Amazon's Alexa products takes advantage of the Internet of Things to listen to user commands, interpret them, and respond.[86] It is important for technology to be connected to devices, the Internet, and the user. While the concept of the Internet of Things has been recognized for many years, the ability of the legislature to regulate the complexity of so many connections has been difficult due to the many aspects of the Internet of Things.[87]

On May 22, 2019, an act named the "Developing Innovation and Growing the Internet of Things Act" (DIGIT Act) was introduced into the Senate of the United States of America as an effort to regulate and protect data within the Internet of Things.[88] The proposed Act includes a steering committee, which would advise programs that would promote and protect the privacy of individuals using the Internet of Things.[89] This Act would help regulate the process through which Amazon's Alexa, and related products, interpret and respond to user interactions.[90] The Act would implement an agency to resolve the issues that arise from security breaches with Amazon's Alexa and related products.[91]

An earlier proposed bill by the same name was introduced to the Senate on March 1, 2016.[92] Another proposed DIGIT Act was engrossed in the Senate after being introduced on January 10, 2017.[93] On January

---

83. *See* Jacob Morgan, *A Simple Explanation Of 'The Internet Of Things,'* FORBES (May 13, 2014), https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#3e8f709c1d09.

84. *Id.*

85. AWS IoT-Overview, AMAZON, https://aws.amazon.com/iot/ (last visited Nov. 30, 2019).

86. *Id.*

87. *Id.*

88. S. 1611, 116th Cong. (2019).

89. S. 1611, 116th Cong. § (e)(2)(D) (2019).

90. *Id.*

91. *Id.*

92. S. 2607, 114th Cong. (as introduced in Senate, March 1, 2017).

93. S. 88, 115th Cong. (as engrossed in Senate, January 10, 2017).

24, 2017, a version of the DIGIT Act was introduced in the United States House of Representatives.[94]

### *D. Privacy Laws in California*

The state of California has the strictest data privacy law in the country, the California Consumer Privacy Act of 2018 (CCPA),[95] which was approved by the Governor on June 28, 2018. The law goes into effect on January 1, 2020, and will protect personal data by allowing consumers to request the personal information collected by businesses.[96] The Act was created after a breach of personal data at a large California company.[97]

> It came to light that tens of millions of people had their personal data misused by a data mining firm . . . . our personal information may be vulnerable to misuse when shared on the Internet. As a result, our desire for privacy controls and transparency in data practices is heightened.[98]

The Act will provide the people of California with a number of rights to their own personal information and data that is collected by companies and their devices.[99] Despite the attempts at providing legislation to protect consumers and their personal data, there are many issues that arise from Amazon Alexa-enabled devices and their listening technology.

## VI. THE LEGAL ISSUES

### *A. Fourth Amendment and the Expectation of Privacy Inside One's Home*

While a voice-controlled, personal assistant device is useful in its ability to make everyday tasks easier, it also creates a record of the user's interactions, habits, and whereabouts.[100] Where such a record is created, it is possible for law enforcement or others to get a copy of your

---

94. H.R. 686, 115th Cong. (as introduced in House of Representatives, January 24, 2017).

95. CAL. CIV. CODE § 1798.100 (effective Jan. 1, 2020); *See also* Johnson, *supra* note 25.

96. California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.100 (effective Jan. 1, 2020).

97. *Id.*

98. *Id.*

99. *Id.*

100. Boughman et al., *supra* note 16.

device usage through a court order.[101] This was a concern not given much consideration before purchasing the device, until it happened. A 2015 incident made national headlines when law enforcement officers, who were investigating a murder case in Arkansas, seized an Alexa-enabled device and issued a subpoena to Amazon, requesting the data associated with the device.[102] The case brought about new fears, making consumers question if purchasing a voice assistant device changes their expectation of privacy inside their own home. The Arkansas death investigation began after a night of drinking and watching football with friends when a man was found lifeless, face-down in a hot tub.[103]

Amazon was brought into the *State of Arkansas v. Bates*[104] case because a witness recalled music streaming through the device the night before.[105] Understanding how Amazon's Alexa products work, law enforcement considered the possibility that while Alexa was recording its interactions with the group, perhaps it picked up evidence crucial to the murder case.[106] Arkansas prosecutors made two requests to Amazon to obtain the device's recordings. Amazon declined to comply with the search warrant, citing "Amazon objects to overbroad or otherwise inappropriate demands as a matter of course."[107] Ultimately, the prosecutors dismissed the murder charge on account of the reasonable doubt standard.[108] For now, the United States Constitution Fourth Amendment[109] protection against unreasonable search and seizures remains intact against digital voice assistants. Therefore, the expectation of privacy inside one's home does not disappear by welcoming a perpetual listening device into one's home.

Further, the Electronic Privacy Information Center (EPIC) responded to law enforcement's request to Amazon in the Arkansas case, stating "It is unreasonable to expect consumers to monitor their

101. *Id.*

102. Eliott 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/index.html. *See State of Arkansas v. Bates,* Case No. CR-2016-370-2 (Circuit Court of Benton County, Ark. 2016).

103. McLaughlin and Allen, *supra* note 102.

104. Case No. CR-2016-370-2 (Circuit Court of Benton County, Ark. 2016).

105. McLaughlin and Allen, *supra* note 102.

106. *Id.*

107. *Id.*

108. Nicole Chavez, *Arkansas Judge Drops Murder Charge in Amazon Echo Case,* CNN (Dec. 2, 2017), https://www.cnn.com/2017/11/30/us/amazon-echo-arkansas-murder-case-dismissed/index.html.

109. U.S. CONST. amend. IV.

every word in front of their home electronics."[110] Under current law, it seems that consumers of the voice technology embedded in Amazon products should not expect any further privacy than they would when using an online search engine.[111]

In a July 2015 letter to the Federal Trade Commission (FTC), EPIC urged the FTC to safeguard consumer privacy rights.[112] In the letter, EPIC stated that "always on" devices like Amazon's Alexa and other voice-controlled assistants might be in violation of federal wiretap laws.[113] EPIC was concerned with Alexa's recording and processing protocols, which sends information into the cloud and back to Amazon for interpretation and storage. This protocol could be in violation of wiretap laws because of the interception of the private data.[114] EPIC urged the FTC to conduct an investigation into Amazon's Alexa and similar devices because of these features; "Americans do not expect that the devices in their homes will persistently record everything they say. By introducing 'always on' voice recording into ordinary consumer products such as computers, televisions, and toys, companies are listening to consumers in their most private spaces."[115]

### *B. Child Privacy Laws*

Recently, EPIC reported that Senators from Massachusetts, Illinois, Connecticut, and Missouri sent a letter to the FTC to investigate Amazon for a new device marketed to children and potential violations of COPPA.[116] The letter, dated May 9, 2019, stated:

> Voice recognition technology and artificial intelligence tools such as the Echo Dot Kids Edition have the potential to enrich and educate kids . . . But these devices also present significant privacy concerns. The Echo Dot Kids Edition captures not only the voice recordings of

110. McLaughlin and Allen, *supra* note 102. EPIC is an organization located out of Washington D.C., that focuses on the research of privacy and civil liberty issues.

111. Boughman et al., *supra* note 16.

112. Marc Rotenberg, Julia Horwitz, and Alan Butler, *EPIC Letter to the Attorney General and the FTC Chairwoman*, ELECTRONIC PRIVACY INFORMATION CENTER, 1–6 (July 10, 2015), https://epic.org/privacy/internet/ftc/EPIC-Letter-FTC-AG-Always-On.pdf.

113. *Id.* at 1.

114. *Id.*

115. *Id.*

116. *Senators Call for FTC to Investigate Amazon Echo for Kids*, ELECTRONIC PRIVACY INFORMATION CENTER (May 9, 2019) https://epic.org/2019/05/senators-call-for-ftc-to-inves.html; 15 U.S.C. § 6501–6506.

> the children who speak to it, but also vast amounts of their personal information.[117]

The Campaign for a Commercial-Free Childhood (CCFC) also strongly supported the concerns expressed by EPIC in their letter.[118] These interest groups reported that Amazon's kid-friendly product infringed on child privacy laws by keeping recorded interactions indefinitely when it refused to comply with user's requests to delete specific information.[119] To analyze whether Amazon's device violates COPPA, a supporting foundation hired lawyers to look into the technology.[120] The lawyers reported "several potential violations of COPPA," a law that has been in effect for twenty years.[121] These interest groups planned to file a formal complaint against Amazon with the FTC, which alleged that the company did not verify parental consent and recorded personal data, despite user attempts to delete child information stored in the cloud through the device.[122] Additionally, these interest groups focused their efforts to protect child privacy towards Facebook, Inc. and Google.[123]

On June 11, 2019, a class action lawsuit was filed in federal court alleging that "Alexa routinely records and voiceprints millions of children without their consent or the consent of their parents," in violation of the Massachusetts Wiretap Statute and similar laws of Florida, Illinois, Maryland, Michigan, New Hampshire, and Washington.[124] The suit asserts that the class members reasonably expected that their private information shared with Alexa products would remain private.[125] It further alleges that "Amazon's intentional

---

117. Richard Blumenthal, Richard J. Durbin, Josh Hawley, and Edward J. Markey, *Letter to FTC to Investigate Amazon Echo for Kids*, UNITED STATES SENATE, 1–3, 1 (May 9, 2019).

118. *Id.* at 2.

119. Matt Day, *Amazon's Echo for Kids Violated Privacy Law, Advocacy Groups Say*, BLOOMBERG (May 9, 2019), https://www.bloomberg.com/news/articles/2019-05-09/amazon-s-echo-for-kids-violated-privacy-law-advocacy-groups-say.

120. *Id.*

121. *Id.*

122. *Id.*

123. *Id.*

124. Hall-O'Neil v. Amazon.com, Inc., 2:19-cv-00910-RAJ-MLP, Document 1, 1–15, 2 (June 11, 2019). *See* MASS. GEN. LAWS CH. 272, § 99 (LexisNexis 2019); Fla. Stat. § 934.03; 720; 720 ILL. COMP. STAT. ANN. 5/14-2 (LexisNexis 2019); MD. CTS. & JUD. PRO. § 10-402 (2019); MICH. COMP. LAWS SERV. § 750.539c (LexisNexis 2019); N.H. REV. STAT. § 570-A:2 (LexisNexis 2019); 18 PA. CONS. STAT. § 5703(2019); WA REV. CODE. ANN. § 9.73.030 (LexisNexis 2019).

125. *Hall-O'Neil*, *supra* note 124, at 12.

and unlawful recording violated Plaintiff's and the Class members' right to privacy in their confidential communications."[126] The suit also addresses an important issue with Amazon's protections for children, the fact that Alexa-enabled devices activate in response to any individual who utters the wake word.[127] Accordingly, the consumer may have consented to the privacy policy that Amazon provides and be placed on notice, but other individuals who interact with the device did not. The class action suit suggests that Amazon warn unregistered users of their ability to be recorded.[128] Crucial to this suit, Amazon records each person who activates the device with the wake word, regardless of whether they are children.[129] The issues addressed here speak to a large concern of the public, that children are more vulnerable, and therefore, their private information should be more protected.

## VII. EUROPEAN PRIVACY LAWS

The European Union recently implemented the strictest data protection regulations in the world in order to protect the individuals of their Union known as the General Data Protection Regulation (GDPR). "The aim of the GDPR is to protect all EU citizens from privacy and data breaches in today's data-driven world."[130] After much debate, the GDPR was approved by the EU Parliament on April 14, 2016 and enforced on May 25, 2018.[131] The new regulation was created to protect the data privacy of EU citizens, as well as to review the data policies of organizations.[132]

The GDPR is known for its wide scope and heavy regulations. It extends to any company that processes data within the Union, regardless of where the company is located.[133] The maximum fine an organization can receive for a violation of the GDPR is 4% of its annual global turnover or twenty million euros.[134] For data breaches,

126. *Id.* at 13.

127. *Id.* at 8.

128. *Id.* at 9.

129. *Id.*

130. *GDPR Key Changes*, EU GDPR, https://eugdpr.org/the-regulation/ (last visited Oct. 27, 2019).

131. *GDPR FAQs*, EU GDPR, https://eugdpr.org/the-regulation/gdpr-faqs/ (last visited Oct. 27, 2019).

132. *Id.*

133. *Id.*

134. *GDPR Key Changes*, *supra* note 130.

organizations can be fined 2%.[135] The new regulation focuses on consumer consent, requiring that "[c]onsent must be clear and distinguishable from other matters" and companies cannot "use long illegible terms and conditions full of legalese."[136]

Further, the GDPR requires that companies notify individuals within seventy-two hours of a breach of their personal data.[137] Additionally, in an effort to increase transparency, organizations must notify individuals of their data being processed and provide free, electronic copies of their personal data upon request.[138] The GDPR also highlights data minimization by calling for data controllers to only process data that is "absolutely necessary for the completion of its duties."[139] The regulation also provides for the appointment of a Data Protection Officer to ensure compliance.[140] While the European regulation is more strict than the data privacy laws in the United States, the GDPR hopes "that companies that operate internationally ensure all of their global audience is GDPR compliant to meet stringent data regulations in the future."[141]

The current state of the law in the United States seems to leave gaps in data security for individuals that actively participate in voice-controlled, personal assistant devices like Amazon's Alexa, especially in comparison to the GDPR. The next section of this Article analyzes the related personal privacy concerns and the current state of the law, and then proposes ways to protect consumers from these devices that perpetually listen inside one's personal life.

## VIII. ANALYSIS

### *A. Learning Technology: The Basics*

Stripped of all the fancy language, the basics of Amazon's Alexa and its learning technology result in one scary thought: eavesdropping. Essentially, consumers buy an Alexa-enabled device, place it in their home, and share personal information with that device. Only the personal information does not stay confined within the device's aesthetically pleasing heap of hard plastic; instead, the information is transmitted through the mysterious cloud. From the cloud that

135. *GDPR FAQs*, *supra* note 131.
136. *GDPR Key Changes*, *supra* note 130.
137. *Id.*
138. *Id.*
139. *Id.*
140. *Id.*
141. *GDPR FAQs*, *supra* note 131.

information is recorded, then listened to by Amazon employees and transcribed for a written record of the user's interactions. This description of the company's recording and listening process seems to be in violation of U.S. federal wiretap laws. Except Amazon, and related companies, describe their processes as "learning technology": a process necessary to improve the device's interaction with users for increased ease and personalization. Accordingly, this process falls under an exception to the federal wiretap laws since the company uses the information to improve the user's interaction.[142] But therein lies another problem. While the device is programmed to record only after hearing the wake word, there have been multiple reports of the device activating after "false positives," as described by Amazon.[143] This means that although unintentional, the device recorded information that the user did not intend to be shared with the device, let alone company employees tasked with listening intently. Furthermore, the company is not prepared for such instances. Based on the idea of learning technology, the device and associated employees are interpreting this information and continuing the necessary process in order to improve the user's interaction.

The main concern with Amazon's Alexa and its learning technology is its impact on the notion of privacy within one's home. People feel safe inside their homes, comforted by their privacy. Because of Alexa's perpetual listening features and past instances of "false positives," introducing an Alexa-enabled product into a home might eliminate part of that safe zone.

### *B. What's Next for Privacy Laws in the United States?*

The closest thing the United States has to the strict regulations and personal data protections in the European Union (EU), is California's Consumer Privacy Act of 2018.[144] However, California's legislation is still not as strict as the GDPR. Further, the Act will not be enacted in California until 2020, so the effectiveness and implications of such strict data regulations in America are not yet known. The anticipated successfulness of the CCPA will likely encourage consumers to support further regulations in other U.S. regions, and perhaps, encourage legislators to set a national regulation regarding individual data privacy.

---

142. *See* 18 U.S.C. § 2511(2)(a)(i).

143. *See* Liao, *supra* note 42.

144. CAL. CIV. CODE § 1798.100 (effective Jan. 1, 2020).

In the United States, data privacy is regulated by different state and federal rules, but there is no broad authority that protects all citizens.[145] But as consumers' privacy concerns increase, will that change? The creation of a main authority for regulating data privacy in the U.S. would take many years and the implementation of California's law is the first step in the right direction. It is unfortunate that only future data breaches are likely to encourage consumers to support such strict regulations.

Currently, the EU's GDPR is reaching across the pond and affecting American corporations by imposing fines for these companies when they violate the regulations regarding consumers located in the Union. However, the strict rules cannot be enforced to protect U.S. citizens. Yet, in order to comply with the GDPR, these companies should be updating its processes and policies to better protect the personal data of individual consumers. Therefore, the strict regulation of the EU may have a ripple effect to protect American consumers because of the widespread changes these large companies will have to make in order to be compliant.

The other option that large corporations have available in response to the GDPR is to pay fines, specifically a maximum of 4%.[146] For companies like Google, Facebook, and others, they pay the fine for security breaches and other violations, rather than make important changes to its data processing infrastructure. Such actions result in continuous problems in the world of data privacy.

Earlier, this Article discussed the proposal of a recent bill, the DIGIT Act, which would serve to regulate the Internet of Things. Legislation, like this proposal, to place stricter standards on big companies and their processing of consumers' private data could be a step towards a widespread regulation of the Internet of Things in the United States. However, as the prior versions of the DIGIT Act have failed, it is likely that the newest proposal will also be unsuccessful. But this begs a more important question of why these proposals are unsupported. Perhaps U.S. consumers are not overwhelmingly concerned with the security of their personal data. Yet the example scenarios of privacy breaches throughout this Article depict a serious issue that should cause concern.

---

145. Derek Hawkins, *The Cybersecurity 202: Why a Privacy Law Like GDPR Would be a Tough Sell in the U.S.*, THE WASHINGTON POST (May 25, 2018), https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/05/25/the-cybersecurity-202-why-a-privacy-law-like-gdpr-would-be-a-tough-sell-in-the-u-s/5b07038b1b326b492dd07e83/.

146. *GDPR Key Changes*, *supra* note 130.

It seems that the best avenue for changing these recording processes of large American corporations is going to be through U.S. child privacy laws. While consumers, whose personal information was breached, are currently without legal action, attorneys are fighting against the recording processes of these devices for the children. Because of the vulnerability associated with children, there are stricter laws regarding the ability to share the personal information of children.

### *C. Can a Perpetual Listening Device be a Good Thing?*

Although these voice-controlled, personal assistant devices present valid privacy concerns, could such an "invasion of privacy" be good? For example, in the Arkansas murder case, if the device captured a key piece of evidence it could have shed light on the death investigation. Additionally, two Amazon employees were distressed to hear a recording that they believed to be a sexual assault.[147] Similarly, imagine two burglars breaking into your home and stealing one of your prized possessions. During the burglary, one of the suspects accidentally activated your Alexa device so the interaction was recorded, containing personal information that could identify the unknown suspect. The ability to have a copy of this voice recording or a transcript of the interaction from Amazon could be increasingly helpful in determining the suspect and recovering your prized possession. In these instances, such interceptions of private conversations could better protect individuals. But then, where would we draw the line? This creates a reasonable dilemma because while consumers do not want their private lives intercepted and recorded, they might prefer it when it could be helpful.

### *D. What Does All of this Mean for Consumers?*

Ultimately, the protection of personal private data rests dually in the hands of the user and the parent company of these voice-controlled, personal assistant devices. While consumers "have been conditioned to the [assumption] that these machines are just doing magic machine learning . . . the fact is[,] there [are] still manual processes involved."[148]

The previously mentioned, Internet of Things, brings about a large concern for the privacy of consumers. The idea that Amazon's voice-controlled assistant is recording and processing data from a

147. Tobin, *supra* note 77.

148. Day et al., *supra* note 61 (quoting Florian Schaub, a professor at the University of Michigan, "[y]ou don't necessarily think of another human listening to what you're telling your smart speaker in the intimacy of your home").

variety of connected devices translates to an intense compilation of an individual's personal data. For example, if one's Alexa-enabled device is connected to one's thermostat, personal contacts, bank accounts, televisions, and alarm systems, then Amazon has a record of each of one's interactions with those devices. Such a record contains personal information that a consumer never expected, nor planned to be shared with others. Yet, there have been examples of personal data breaches that made national headlines simply because of the depth of personal information leaked from these records. Remember the Amazon files delivered to the wrong recipient in mid-2018 mentioned above?[149] In that example, an investigator discovered the true identity of the Alexa user, using only his record of interactions with the device sent by Amazon. This means that absolute strangers listened to the personal details of another's daily interactions with his Alexa device to make real-world connections to the actual owner of the information.

### *E. How Should You as a Consumer Protect Your Data?[150]*

The voice assistant's key learning technology requires that the device stays in a perpetual listening mode, awaiting a user's command. This feature requires its user to be alert and able to recognize that once the device is triggered, a private conversation is no longer private.

Amazon gives the option to alter the wake word, which is factory set as "Alexa." This signal may be problematic for users whose name, friend's name, or family name resembles the wake word. But, making a change to your wake word could be an easy fix to situations of "false positives" during private conversations.

Additionally, Amazon's Alexa-enabled devices, like the Echo, include a microphone-off button, which inhibits the listening device. This feature seems like the safest way to control your personal data; however, it could change your habitual usage with the device. One would have to remember to switch the device back on for it to fulfill any requested action. Similarly, users could unplug the device to avoid mishaps of "false positives." However, this type of solution is ineffective for consumers that wish to use the device's features unless the consumer takes the affirmative step to plug-in the device for each use.

---

149. *See* Bleich, *supra* note 47.

150. *See* O'Flaherty, *supra* note 61 (stating "smart home devices add convenience to your life but they also come with significant security risks. If you are going to use them, make sure you lock them down as much as possible to keep your private data safe.").

## IX. CONCLUSION

While there are many problems and privacy concerns that remain surrounding Amazon's Alexa, and related personal assistant devices, the current climate of U.S. lawmakers are not yet ready to make changes for more regulations. Therefore, this places a heavy burden on consumers to be cautious about the information they share with these devices. The devices absorb the personal information of its user to assist with daily activities. Many of the issues discussed throughout this Article have existed since the creation of voice-controlled, personal assistant devices years ago, yet they still continue today. One might even suggest that those issues are more severe today because of the increasing wingspan of the Internet of Things. Ultimately, it seems that the responsibility of protecting one's personal information lies with the consumer themselves. Anyone who uses an Amazon Alexa-enabled device, or similar product, is using them at their own risk.

**Marissa Merrill**