Hofstra Law Review

Volume 49 | Issue 3 Article 7

3-1-2021

"Hey Siri, What Does the Government Know About Me?": Increasing the Volume on Smart Speaker Awareness

Jacob A. Manzoor
Maurice A. Deane School of Law at Hofstra University

NOTE

"HEY SIRI, WHAT DOES THE GOVERNMENT KNOW ABOUT ME?": INCREASING THE VOLUME ON SMART SPEAKER AWARENESS

I. INTRODUCTION

"Hey Alexa, play my favorite music."[1] Smart speakers[2] have a wide variety of capabilities.[3] By connecting the home to the Internet, users are able to ask the device to do anything from playing music, to locking the doors, to lowering the temperature in the home.[4] It is estimated that as of the end of 2019, there were over ninety million smart speakers in the United States and over 200 million smart speakers worldwide.[5] In fact, smart speaker usage is set to overtake tablet use by 2021.[6]

1. *See generally Alexa Features Help*, AMAZON, https://www.amazon.com/gp/help/customer/display.html (last visited Apr. 1, 2021) (explaining the commands used to get the attention of Amazon's smart speaker and virtual assistant, Alexa). Alexa is capable of referencing the user's prior music selections and playing songs that the speaker believes are the user's favorite. *Id.* "Alexa" is the wake word for the Amazon smart speaker that triggers the recording, which is sent to the cloud. *Id.* Alexa is able to speak, comprehend, and complete the user's commands. *Id.* Alexa is programmed to be able to play music, order through Amazon.com, and dim the lights, among other functions. *Id.*

2. A smart speaker is a voice-controlled compact device placed within one's home that can connect the home to the Internet and complete a variety of tasks as directed by the user, such as raising the volume, checking the weather, or playing music. Robert Silva, *What Is a Smart Speaker?*, LIFEWIRE, https://www.lifewire.com/smart-speaker-4145037 (Dec. 2, 2020).

3. *See id.*

4. *Id.*

5. *See* Robert Williams, *Smart Speakers to Top Tablet Use by 2021, Forecast Says*, MARKETING DIVE (Apr. 16, 2019), https://www.marketingdive.com/news/smart-speakers-to-top-tablet-use-by-2021-forecast-says (explaining the rapid growth in popularity of smart speakers and the total number of smart speakers expected to be in homes by 2023); Steve Ranger, *End of an Era: Soon Smart Speakers Will Outnumber Tablets*, ZDNET (Apr. 15, 2019, 6:59 AM), https://www.zdnet.com/article/end-of-an-era-soon-smart-speakers-will-outnumber-tablets.

6. Ranger, *supra* note 5 (explaining how smart speakers have become increasingly popular in the United States and around the world).

Although these devices can provide modern conveniences, they can also intrude on one's privacy by listening to one's conversations.[7] If asked directly if it is listening *all the time*, the device will generally return an answer along the lines of, "I only record and send audio back to the Amazon cloud when you say the wake word."[8] However, according to cybersecurity experts, smart speakers may be recording conversations even when one does not directly or intentionally use the "wake word."[9] It is estimated that in the course of a ten-minute conversation, a smart speaker may mishear ten to thirty words, which may cause the device to begin recording at any time.[10] Although all of the giant technology (or "tech") companies, including Apple, Amazon, and Google, give assurances that customer data is kept safe and is not given out freely to third parties, these assurances ring hollow in the day and age of constant security breaches and demand for consumer information.[11]

Consumers are also growing increasingly aware of the fact that smart speakers may be listening to their conversations and recording them.[12] Nevertheless, smart speaker sales continue to rise.[13] The growing awareness of the risk of being recorded is likely why some jurisdictions are creating regulations to try to stop tech companies from keeping consumer's private data and using it for their own benefit.[14]

The cause for concern is even greater when it comes to the government's ability to access the data collected by smart speakers.[15]

---

7. *See How Creepy Is Your Smart Speaker?*, ECONOMIST (May 11, 2019), https://www.economist.com/leaders/2019/05/11/how-creepy-is-your-smart-speaker (explaining that the conveniences of smart speakers come with the cost that they may be listening in to your conversations and compromising your security).

8. *Id.*

9. Jen Monnier, *Your Smart Speaker Records You More Often Than You Think*, SCIENCELINE (Apr. 20, 2018), https://scienceline.org/2018/04/smart-speaker-records-often-think.

10. *Id.*

11. Hugh Langley & Jennifer Pattison Tuohy, *Smart Home Privacy: What Amazon, Google and Apple Do with Your Data*, AMBIENT (Nov. 8, 2019), https://www.the-ambient.com/features/how-amazon-google-apple-use-smart-speaker-data-338; *see generally* Dan Swinhoe, *The 15 Biggest Data Breaches of the 21st Century*, CSO (Jan. 8, 2021, 2:00 AM), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html (listing the largest data breaches that have occurred in the twenty-first century and explaining how many consumers were impacted).

12. Allison Ingersoll, *Users Worry About Smart Speaker Privacy, But Keep On Buying Them*, BLOOMBERG (Sept. 5, 2019), https://www.bloomberg.com/news/articles/2019-09-05/users-worry-about-smart-speaker-privacy-keep-on-buying-them.

13. *Id.*

14. *See id.*

15. Trevor Timm, *The Government Just Admitted It Will Use Smart Home Devices for Spying*, GUARDIAN (Feb. 9, 2016, 3:29 PM), https://www.theguardian.com/commentisfree/2016/feb/09/internet-of-things-smart-devices-spying-surveillance-us-government (discussing how the U.S.

The data collected by smart speakers can be used by the government to get a detailed look at one's homelife.[16] In fact, recordings obtained by the government from an Amazon Echo were used as evidence in the State of Arkansas' case to support a first-degree murder charge.[17] While some states have taken action on wider cybersecurity and data privacy concerns, they do not specifically regulate smart speakers and, more importantly, what information the government can access from these smart speakers without a warrant.[18]

The laws passed range from extensive privacy and cybersecurity reform, as in California, to simple reactive laws instructing companies what to do once a data breach has occurred.[19] This range in regulation on a state-by-state basis creates hurdles and inefficiencies for corporations by having to potentially comply with up to fifty different statutes and guidelines.[20] Furthermore, this patchwork of regulation does little to protect consumers' private data and gives them very few, if any, options to limit the data that is gathered by technology companies.[21] Much of this data can simply be passed onto the government, without a warrant, to further a prosecutor's case.[22] It is for this reason that smart speakers

---

government indicated that it would use data gathered from devices connected to the "Internet of things" ("IoT") to gather intelligence). This Note defines the IoT as the many devices, like thermostats, cameras, and other appliances, that are connected to the Internet via smart devices. *See infra* notes 74-80 and accompanying text.

16. *See* Timm, *supra* note 15.

17. State v. Bates, No. CR20160370, 2016 WL 7627013 (Ark. Cir. Sept. 7, 2016); Colin Dwyer, *Arkansas Prosecutors Drop Murder Case that Hinged on Evidence from Amazon Echo*, NPR (Nov. 29, 2017, 5:42 PM), https://www.npr.org/sections/thetwo-way/2017/11/29/567305812/arkansas-prosecutors-drop-murder-case-that-hinged-on-evidence-from-amazon-echo.

18. *See Virtual Home Assistants and the Laws and Regulations Struggling to Keep Up with the Times*, IE EXPONENTIAL LEARNING (Jan. 23, 2019), https://www.ie.edu/exponential-learning/blog/business/virtual-home-assistants-laws-regulations-struggling-keep-times (explaining that while some states have passed general cybersecurity laws, there are no laws directly regulating smart speakers); John Adams, *A Seismic Shift: What California's New Privacy Law Means for Cybersecurity*, SEC. MAG. (July 5, 2018), https://www.securitymagazine.com/articles/89201-a-seismic-shift-what-californias-new-privacy-law-means-for-cybersecurity; *see also* Benjy Schirm, *Smart Speakers and the Violation of Our Civil Rights*, SUPER LAWS. (Feb. 7, 2021), https://www.superlawyers.com/united-states/article/smart-speakers-and-the-violation-of-our-civil-rights/00643e59-f7b3-4b34-b364-0f802635da9d.html.

19. *See* Adams, *supra* note 18 (explaining the extent of the newly-passed California cybersecurity law).

20. *See* Taylor Armerding, *Awash in Regulations, Companies Struggle with Compliance*, SYNOPSYS (Sept. 10, 2019), https://www.synopsys.com/blogs/software-security/regulatory-compliance-challenges (explaining the difficulties of many companies when trying to comply with new cybersecurity and data privacy regulations).

21. Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN REL. (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection.

22. *See* Schirm, *supra* note 18.

pose a particularly important data privacy risk as the data they collect pierces metadata[23] and allows the government to access the actual raw data collected by smart speakers.[24]

This Note will begin by explaining the issues surrounding why smart speakers are unlike other types of smart devices and why they pose a particular threat to an individual's right to privacy.[25] Part III will then discuss the history of the Fourth Amendment right to privacy, particularly its evolution from protecting against common law trespass to a broader right of privacy.[26] Part IV proposes that the U.S. Supreme Court grant certiorari on a case involving smart speakers.[27] The hope would be that the Supreme Court would expand upon all citizens' Fourth Amendment privacy rights to explicitly include data collected by smart speakers and to make it impermissible for the government to obtain such information without a proper warrant.[28]

II. WHY SMART SPEAKERS POSE A PARTICULAR THREAT THAT IS IN NEED OF ACTION

This Part will discuss what kind of information is collected by smart speakers as well as the quantity of data collected by these devices and what makes this information different from other types of data that warrant Fourth Amendment protection against unjustified government access.[29] Subpart A will discuss what kind of information is gathered by smart speakers.[30] Subpart B will go on to discuss why smart speakers pose a particular issue that should be dealt with accordingly by the Supreme Court.[31]

23. *See* Mike Chapple, *What Is Metadata?*, LIFEWIRE (June 3, 2019), https://www.lifewire.com/metadata-definition-and-examples-1019177. "Metadata is data about data." *Id.* Metadata can give someone an overall, holistic view of larger trends and can generally describe data that is part of the macroeconomic trend. *Id.* Nevertheless, metadata is not the data itself, and although helpful, metadata does not give you the information about specific individuals or any other specific transactions or interactions. *Id.*

24. *See id.*; Monnier, *supra* note 9.

25. *See infra* Part II.

26. *See infra* Part III.

27. *See infra* Part IV.

28. *See infra* Part IV.

29. *See infra* Part II.

30. *See infra* Part II.A.

31. *See infra* Part II.B.

A. What Information Is Collected by Smart Speakers?

This Subpart will lay out the kinds of information that are gathered by smart speakers.[32] However, to fully understand all of the threats that smart speakers pose, it is important to understand how a smart speaker works.[33] Smart speakers can perform a variety of tasks, from ordering a pizza to informing you what the weather is going to be like next week, and this is all done through a voice-controlled digital assistant.[34] Many of the big tech companies have their own version of a digital assistant,[35] but they all generally perform the same functions.[36] In order to activate the digital assistant to get it to perform a task, one must first use the "wake word."[37] While many large tech companies claim that their smart speaker is only listening for the "wake word," and only then will the device start recording, this is generally not the case because smart speakers often mishear words and begin recording conversations without the knowledge of the user.[38]

Smart speakers are constantly listening to conversations and are collecting data that is being transmitted to servers which store this information.[39] The kinds of information being collected by smart speakers are vast and can range from location data to actual recordings of one's voice conversations.[40] Generally, downloading applications ("apps")—like Tinder, LinkedIn, and Facebook—onto a phone allows these tech companies to collect and store data so that they can target advertisements and align an individual's feed with targeted messaging that these companies believe that the individual might be interested in.[41] Similarly, on smart speakers, users can use apps that they have downloaded via their virtual assistant.[42] These apps all include terms and

32. *See infra* Part II.A.

33. *See* Emma Stenhouse, *Smart Speakers — How Do They Work?*, EVOLVING SCI. (Nov. 15, 2017), https://www.evolving-science.com/intelligent-machines/smart-speakers-how-do-they-work-00483.

34. *See id.*; Silva, *supra* note 2.

35. Parker Hall & Jeffery Van Camp, *The Best Smart Speakers with Alexa, Google Assistant and Siri*, WIRED (Nov. 26, 2020, 8:00 AM) https://www.wired.com/story/best-smart-speakers (explaining the different types of assistants found in smart speakers and their various features).

36. *Id.*

37. Monnier, *supra* note 9.

38. *See id.*

39. Langley & Tuohy, *supra* note 11 (explaining how data is gathered and stored on tech company servers). It is important to note that, by default, smart speakers do not store or send audio unless activated with the chosen "wake word." *See id.*

40. Tom Calver & Joe Miller, *What Tech Giants Really Do with Your Data*, BBC NEWS (July 5, 2018), https://www.bbc.com/news/business-44702483.

41. *Id.*

42. *See, e.g.*, *Alexa Features Help*, *supra* note 1.

conditions to ensure that the user is bound by the app's rules while using the platform; however, oftentimes people do not even read the terms.[43] These terms allow companies like Facebook to keep a user's search history, even after it has been "deleted."[44] Moreover, Facebook is not the only company that does this: Amazon has also been known to hold onto smart speaker data even after it has been "deleted."[45] As discussed in Part IV, these policies used by tech companies give rise to privacy and cybersecurity issues that need to be addressed with a comprehensive and national solution to the issue.[46]

Furthermore, not only might conversations be recorded while the individual is unaware, but there also may be a human analyst from Amazon, Apple, or Google listening in on that person's conversation.[47] Each of the three largest smart speaker companies acknowledges that there are human analysts listening in on some conversations, and their rationale is that it helps the company to improve speech recognition.[48] While these companies claim that there is no personally identifiable information being transmitted to analysts with the recordings, the voices are not always changed.[49]

Therefore, the analyst is reviewing raw data that pierces the metadata and is able to access the unadulterated recordings.[50] What is even more alarming is that there is no setting that can disable human analysis of these recordings, and there is no prominent disclaimer in which individuals are told that their conversations may be monitored, recorded, or reviewed.[51] Furthermore, there is no law prohibiting any of these technology companies from turning over these recordings to the government.[52] Currently, the only protection against government access

43. *See* Calver & Miller, *supra* note 40.

44. *Id.* (explaining that while Facebook offers an option to delete one's search history, Facebook oftentimes holds on to a user's deleted search history for up to six months).

45. Makena Kelly & Nick Statt, *Amazon Confirms It Holds On to Alexa Data Even if You Delete Audio Files*, VERGE (July 3, 2019, 4:14 PM), https://www.theverge.com/2019/7/3/20681423/amazon-alexa-echo-chris-coons-data-transcripts-recording-privacy (explaining that Amazon has admitted to holding on to users' personal data, even after it has been "deleted" by the user).

46. *See infra* Part IV.

47. *See Smart Speaker Recordings Reviewed by Humans*, BBC NEWS (Apr. 11, 2019), https://www.bbc.com/news/technology-47893082.

48. *Id.*

49. *See id.*

50. *See id.*; *see also* Chapple, *supra* note 23.

51. *See Smart Speaker Recordings Reviewed by Humans*, *supra* note 47.

52. *See Cooperation or Resistance?: The Role of Tech Companies in Government Surveillance*, 131 HARV. L. REV. 1722, 1722, 1728 (2018) (explaining how the tech companies themselves decide whether or not to cooperate or resist the requests from the government for

to these recordings comes from the tech companies themselves who created the smart speakers.[53]

B. *What Makes the Information Gathered by Smart Speakers Unique?*

This Subpart will discuss why smart speakers pose a unique threat that needs to be addressed more urgently than general privacy concerns involving other kinds of smart devices.[54] Smart speakers pose a particular threat to an individual's right to privacy because they are constantly listening and transmitting actual data to servers.[55] Smart speakers can and do record intimate conversations in the homes of Americans.[56] The data collected by smart speakers during these conversations is instantly accessible to tech companies, and the government faces a low bar in obtaining this information for prosecutorial purposes unless they face pushback from the tech companies themselves.[57] By piercing the metadata, smart speakers give the actual data of individuals to anyone who reviews the recordings by being able to listen to the person's voice, usually unaltered, albeit the tech companies claim human reviewers never receive identifying information or location data.[58]

Recently, this concern has been brought to the forefront of media attention in the case of *State v. Bates*,[59] a homicide case that concerned whether the Arkansas State government could access recordings made by an Amazon Echo smart speaker.[60] Mr. Bates was charged with the murder of one of his friends, who, after a night of drinking and watching football, was found by Mr. Bates floating unconscious face down in his hot tub.[61] Mr. Bates's home was equipped with an Amazon Echo smart

---

individuals' personal data. During the aftermath of September 11, 2001, some tech companies were particularly cooperative with government requests for sensitive data of individuals.).

53. *See* Schirm, *supra* note 18 (explaining that there are no protections from the government and the only consumer protections that exist are those protections given by the tech companies themselves).

54. *See infra* Part II.B.

55. *See supra* note 39 and accompanying text; ARI EZRA WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE 142-43, 145 (2018).

56. *See* WALDMAN, *supra* note 55.

57. *See* Schirm, *supra* note 18.

58. *Smart Speaker Recordings Reviewed by Humans*, *supra* note 47.

59. No. CR20160370, 2016 WL 7627013 (Ark. Cir. Sept. 7, 2016).

60. Elliott C. McLaughlin, *Suspect OKs Amazon to Hand Over Echo Recordings in Murder Case*, CNN (Apr. 26, 2017, 2:52 PM), https://www.cnn.com/2017/03/07/tech/amazon-echo-alexa-bentonville-arkansas-murder-case/index.html.

61. *Id.* Mr. Bates invited two friends over to his home to watch football and have a few drinks. *Id.* After having a shot of vodka and some beer, the group decided to get into Mr. Bates's hot tub and around 1:00 AM. Bates left the two friends and went to bed. *Id.* When he woke up the next morning, he saw that one of his friends was floating face down in the hot tub. *Id.* At the time of his

speaker, and the prosecution believed that the information gathered by the smart speaker, particularly the voice recordings, would prove Mr. Bates's guilt.[62] Amazon initially refused the prosecutor's request for the recordings from the Echo, citing customer privacy concerns.[63] Nevertheless, Mr. Bates himself wanted Amazon to turn over the recordings as he believed it would prove his innocence, and Amazon eventually did turn over the recordings to prosecutors.[64] After the prosecutors received the recordings and analyzed them, they moved to dismiss the charges against Mr. Bates.[65]

Although the information captured by the Amazon smart speaker tipped in favor of Mr. Bates here, there are times when information captured by smart speakers can seemingly incriminate individuals.[66] Moreover, the prosecution of Mr. Bates shows that consumers are currently left solely at the will of tech companies and their individual privacy policies, leaving tech companies with the final say as to whether or not consumer data and private information is shared with the government.[67] Alarmingly, not all tech companies have strong privacy policies, and the ones that do, like Apple, reserve the right to change their policies at any moment.[68] The difference in policies among tech companies is significant: Apple claims that data privacy should be a protected and fundamental human right,[69] whereas Google freely sells

---

death, the friend, Mr. Collins, had a blood alcohol content of .32, which is four times the legal limit to drive in Arkansas. *Id.* Prosecutors filed charges against Bates for murder, as they believed that they had strong circumstantial evidence of an attempted cover-up—the fact that there was unusually high water usage after the murder took place. *Id.* Upon finding out that Mr. Bates had an Amazon Echo, the prosecutors pursued the recordings from the device in an effort to obtain direct evidence that Bates committed the crime. *Id.*

62. *Id.*

63. Dwyer, *supra* note 17.

64. *Id.*

65. *Id.*

66. *See id.*

67. *See id.*

68. *See Our Privacy Policy*, APPLE, https://www.apple.com/privacy (last visited Apr. 1, 2021).

69. *Id.*; Ben Popken, *Google Sells the Future, Powered by Your Personal Data*, NBC NEWS (May 10, 2018, 4:30 AM), https://www.nbcnews.com/tech/tech-news/google-sells-future-powered-your-personal-data-n870501. Notably, Apple refused to unlock the phone of the suspected San Bernardino shooter when the Government tried to gain access to his personal data from an iPhone that he used. Ellen Nakashima, *Apple Vows to Resist FBI Demands to Crack iPhone Linked to San Bernadino Attacks*, WASH. POST (Feb. 17, 2016), https://www.washingtonpost.com/world/national-security/us-wants-apple-to-help-unlock-iphone-used-by-san-bernardino-shooter/2016/02/16/69b903ee-d4d9-11e5-9823-02b905009f99_story.html. The Government wanted Apple to create a new software to give government prosecutors a "backdoor" into the suspected shooter's personal information. *Id.* Apple refused, citing broad cybersecurity concerns as well as concerns for the individual's privacy rights. *Id.* Litigation ensued, and while there was no final decision on the merits because the Government was able to gain access to the information by

consumers' private data to third-parties in order to tailor ads and increase its revenue.[70]

The *Bates* case is just one instance demonstrating how the government has an interest in obtaining data from smart speakers.[71] Other government officials, including former New York City Police Department Commissioner William J. Bratton and former National Counterterrorism Center Director Matt Olsen, have openly stated that the public interest in a case is often great enough for the government to obtain access to personal data collected by smart devices.[72] The fact that government officials are not only interested in the personal data of individuals from smart speakers and other smart devices, but are also actively seeking such information, as in the *Bates* case, shows how the threat to privacy is persistent, real, and needs to be addressed.[73]

Another reason why smart speakers pose a particular threat if their data is freely accessed by the government is that they are connected to the "Internet of things" ("IoT").[74] The IoT is essentially the collection of

---

another means, this transaction shows Apple's commitment to consumer privacy and the protection of consumers' personal data. Matt Zapotosky, *FBI Has Accessed San Bernardino Shooter's Phone Without Apple's Help*, WASH. POST (Mar. 28, 2016), https://www.washingtonpost.com/world/national-security/fbi-has-accessed-san-bernardino-shooters-phone-without-apples-help/2016/03/28/e593a0e2-f52b-11e5-9804-537defcc3cf6_story.html. The Government's tenacity to get the data from the San Bernardino shooter's iPhone, even against the will of Apple, proves that the Government is willing to go to great lengths to obtain the personal information of the individuals that it is trying to prosecute. *See id.* The Government's persistence in the San Bernardino case illustrates why it is important that Fourth Amendment protection be extended to one's personal data captured by smart devices—in particular, data obtained via smart speakers. *Id.*; *see infra* Part IV.

70. Popken, *supra* note 69. Google is known for its search engine, but it also has a variety of different products, such as Google's own free version of Microsoft's suite of office software entitled "Google docs." *See id.* Google offers many different free services and free software products to consumers, but in return for getting a free product, Google reserves the right to collect data from the consumers that use its products. *Id.* Google, in turn, uses this data to market more of its products to those consumers, but Google also sells some of the data that it obtains to third parties so that those third parties can tailor various advertisements to consumers that are the most likely to purchase those products. *Id.* While there may not be an incentive for Google to turn over vast amounts of data to the government for free, there is a concern that Google would hand over the information to the government for the right price. *See id.* This is alarming in and of itself, as the government may already be one of Google's many customers purchasing consumer data for its own purposes, and the public would not know. *See id.* Even if the government is not a current customer purchasing data from Google, there is nothing stopping the government from doing so, just as any other third party might in the future. *Id.*

71. *See* McLaughlin, *supra* note 60.

72. Nakashima, *supra* note 69.

73. *See id.*

74. Sara Sorcher, *The Technology 202: Alexa Are You Spying on Me? Here's Why Smart Speakers Raise Serious Privacy Concerns*, WASH. POST (May 6, 2019, 9:20 AM), https://www.washingtonpost.com/news/powerpost/paloma/the-technology-202/2019/05/06/the-

devices that are connected to or that are able to connect to the Internet that can communicate data to each other in a common language.[75] The IoT is expanding rapidly and encompassing more and more devices each year.[76] Any device that has the capability of connecting to the Internet has the ability to be part of the IoT.[77] The IoT also includes parts of larger devices, such as the engine of an airplane or the drill of an oil rig.[78] The IoT is helpful to consumers and manufacturers as it allows devices to communicate the data that they collect to one main server and maintains the ability to interact with other connected devices.[79] The IoT is particularly powerful when combined with a device like a smart speaker that can be connected to a wide variety of devices that are also connected to the IoT.[80]

A smart speaker that is connected to the user's schedule, smart home, and the IoT can provide real-time updates based on different weather or traffic conditions.[81] If a person connects all of their devices and links them with their smart speaker, it can make that person's life easier by adapting to changing conditions seamlessly.[82] For example, a smart speaker that is connected to the IoT and communicates with other devices is able to recognize when there is heavier traffic than usual on the route to work and is thus able to set the person's alarm to go off earlier, giving the person ample time to make it to their early morning meeting.[83]

The fact that a smart speaker can communicate with other devices connected to the IoT poses a particular privacy risk because if the government can freely—either with a warrant or without a warrant—gain access to the data collected by a smart speaker, it can also get the data that the smart speaker has collected from a variety of other devices that it communicates with.[84] This is especially troubling since there is

---

technology-202-alexa-are-you-spying-on-me-here-s-why-smart-speakers-raise-serious-privacy-concerns/5ccf46a9a7a0a46cfe152c3c.

75. *See* Jacob Morgan, *A Simple Explanation of 'The Internet of Things,'* FORBES (May 13, 2014, 12:05 AM), https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand.

76. *See id.*

77. *Id.*

78. *Id.*

79. *See id.*

80. *See id.* (explaining that a smart device, such as a smart speaker, can connect to your home, calendar, phone, shopping history, and other devices, giving it the ability to dim the lamp lights, set appointments, call people, and buy items, among other functions).

81. Jen Clark, *What Is the Internet of Things (IoT)?*, IBM (Nov. 17, 2016), https://www.ibm.com/blogs/internet-of-things/what-is-the-iot.

82. *See id.*

83. *Id.*

84. *See* Sorcher, *supra* note 74.

really no limit as to what kinds of other devices smart speakers can be connected with.[85] Through a smart speaker's connectivity to the IoT, the government would be able to access a person's agenda, their daily routine, any messages they send to friends and family, and, with the advent of smart appliances, even what that person has stocked in their refrigerator.[86] Data collected by smart speakers that are connected to the IoT can give an incredibly detailed look into an individual's life and can compromise someone's privacy not only in their own home but also in their potential defenses against the government.[87] James Clapper, Director of National Intelligence, cautioned the potential danger of the government's use of the IoT: "In the future, intelligence services might look to use the [IoT] for identification, surveillance, monitoring, location tracking, and targeting for recruitment, or to gain access to networks or user credentials."[88]

Technology companies use all-too-familiar tactics to pay lip service to the notice requirement to consumers who are buying their products.[89] Choice is limited in the same way, as all major smart speakers have similar terms and conditions pages, and equally so, it would take hours to read and comprehend all of the language inside the documents.[90] Technology companies often keep consumers underinformed about what they are doing with the individual's personal data, and this is precisely why there needs to be a strong and effective solution to the problem, especially as it pertains to companies passing off such information to the government upon request without a valid warrant issued by a judge.[91]

---

85. *See* Timm, *supra* note 15 (explaining how the IoT can connect to various different appliances and devices through a smart speaker, giving the government ample opportunity to get an in-depth look at someone's homelife).

86. *Id.*; *see* Clark, *supra* note 81; Sorcher, *supra* note 74.

87. *See* Timm, *supra* note 15; *see supra* note 86 and accompanying text.

88. Timm, *supra* note 15.

89. *See* Zack Whittaker, *Stop Saying, 'We Take Your Privacy and Security Seriously,'* TECH CRUNCH (Feb. 17, 2019, 7:07 PM), https://techcrunch.com/2019/02/17/we-take-your-privacy-and-security-seriously (discussing how large companies use phrases such as, "we take the privacy of personal information seriously," to quell user fears and detract from liability, rather than to serve as an actual commitment to cybersecurity and privacy concerns).

90. Silvia De Conca, *Between a Rock and a Hard Place: Owners of Smart Speakers and Joint Control*, 17 SCRIPTED 238, 242 (2020) (explaining how the first task for new smart speaker owners is to accept the terms and conditions that come with the device, which seem to be similar for both Google and Amazon); Susan Allen, *Privacy in the Twenty-First Century Smart Home*, 19 J. HIGH TECH. L. 162, 179-80 (2018) (explaining how consumers have no choice when accepting the terms and conditions "because of modern civilization's dependence on smart devices").

91. *See* Schirm, *supra* note 18.

III. THE HISTORY OF THE FOURTH AMENDMENT RIGHT TO PRIVACY

This Part will discuss how the Fourth Amendment has evolved over time to include broader rights as citizens began to demand a more robust expectancy of privacy, and what exactly the Fourth Amendment protections currently offer.[92] Subpart A will discuss the Fourth Amendment's traditional right to privacy.[93] Subpart B will go on to discuss the expansion of the right to privacy up to the current standard today.[94] Subpart C will discuss the Supreme Court's further expansion of the Fourth Amendment to encompass cellphone location data in the case of *Carpenter v. United States*.[95] Subpart D will go on to lay out why legislation from the states cannot adequately solve the issue of government access to data from smart speakers.[96]

A. The Traditional Fourth Amendment Right to Privacy

This Subpart will discuss the traditional Fourth Amendment right to privacy.[97] The Fourth Amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[98]

Traditionally, the Fourth Amendment was interpreted to give protection against common-law trespass.[99] The greatest Fourth Amendment protections were against the government in one's own home.[100] The Supreme Court held that "at the very core [of the Fourth Amendment] stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion."[101] The right to exclude others from intrusion onto private personal property, especially in one's own home, but also in one's vehicle, was and still is held in high regard.[102] While the Court consistently recognized privacy in one's

92. *See infra* Part III.
93. *See infra* Part III.A.
94. *See infra* Part III.B.
95. 138 S. Ct. 2206 (2018); *see infra* Part III.C.
96. *See infra* Part III.D.
97. *See infra* Part III.A.
98. U.S. CONST. amend. IV.
99. *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 809-11 (2004).
100. *Id.* at 811; *see also* Silverman v. United States, 365 U.S. 505, 511 (1961).
101. *Silverman*, 365 U.S. at 511.
102. Kerr, *supra* note 99, at 811-12.

property rights, the Court did allow warrantless surveillance techniques that invaded privacy without invading property.[103] It was not until the Court's decision in *Katz v. United States*[104] that the term *right to privacy* become ingrained within the subtext of the Fourth Amendment.[105]

B. The Current Right to Privacy Under the Fourth Amendment

This Subpart will discuss the current right to privacy that is afforded by the Fourth Amendment.[106] In 1967, the United States Supreme Court decided the case of *Katz*, which created the current test for determining when there is a reasonable expectation of privacy.[107] In *Katz*, the Court held that Mr. Katz had a reasonable expectation of privacy during his phone conversation in a public phonebooth because he had closed the door behind him.[108] The Court wrote, "No less than an individual in a business office, in a friend's apartment, or in a taxicab, a person in a telephone booth may rely upon the protection of the Fourth Amendment."[109]

In his concurrence, Justice Harlan laid out a two-part test used to determine whether or not an individual has a "reasonable expectation of privacy": (1) the individual must have exhibited a subjective expectation of privacy; and (2) that expectation of privacy is deemed reasonable by society.[110] Justice Harlan's test has since become the fundamental test in determining whether or not one has a reasonable expectation of privacy within the confines of a Fourth Amendment analysis.[111] This was a landmark case and a significant change in the law, as now a person's privacy is protected by the Fourth Amendment—not just a particular location.[112] Moreover, *Katz* created a right to privacy against the government that no longer required the government to physically intrude into someone's private residence in order to find protection under the

---

103. *Id.* at 813.

104. 389 U.S. 347 (1967).

105. *See* Allen, *supra* note 90, at 167-68 (explaining how the right to privacy was expanded after the *Katz* ruling, particularly as it pertains to one's person and within one's own home).

106. *See infra* Part III.B.

107. *Katz*, 389 U.S. at 352.

108. *Id.* The closed door was a significant factor in the Court's analysis, as the Court ruled that by closing the door, Mr. Katz signaled that he was having a private conversation that was not open to the public. *Id.*

109. *Id.*

110. *Id.* at 361 (Harlan, J., concurring).

111. *Expectation of Privacy*, LEGAL INFO. INST., https://www.law.cornell.edu/wex/expectation_of_privacy (last visited Apr. 1, 2021).

112. *See* Marc J. Blitz, *Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World that Tracks Image and Identity*, 82 TEX. L. REV. 1349, 1363 (2004).

law.[113] *Katz* was a crucial ruling in the realm of privacy rights, and it provides a strong foundation for the Court to further expand the Fourth Amendment right to privacy.[114]

Another landmark case that expanded Fourth Amendment protections was *United States v. Jones*.[115] In *Jones*, the Supreme Court expanded an individual's right to privacy by ruling that when the government attached a global positing device (GPS) on the individual's car, the government violated the Fourth Amendment as this constituted physical intrusion into one's personal property in order to seize personal information.[116] Although the government physically intruded in this case, both Justice Alito and Justice Sotomayor noted in their concurrences that breach of the Fourth Amendment does not depend on whether there was a physical intrusion.[117]

Plainly stated, "Physical intrusion is now unnecessary to many forms of surveillance."[118] The Justices noted it would be unnecessary and rather foolish to require the government to always physically trespass before Fourth Amendment protections would kick in.[119] In the modern era, where information can be easily obtained through the Internet and other technological advances, the government can trespass against individuals' private rights even without a physical intrusion onto their property.[120] The holding in *Jones* gave the Court the proper framework to hear a case concerning government intrusion of an individual's Fourth Amendment rights without physical intrusion onto their property, and that case was *Carpenter*.[121]

C. *The Expansion of the Fourth Amendment Right to Privacy Under* Carpenter

This Subpart will discuss the further expansion of Fourth Amendment rights to privacy particularly after the decision in

113. Allen, *supra* note 90, at 167.

114. *See* Blitz, *supra* note 112, at 1366.

115. 565 U.S. 400 (2012).

116. *See id.* at 405-06.

117. *Id.* at 414 (Sotomayor, J., concurring); *id.* at 426-29 (Alito, J., concurring).

118. *Id.* at 414 (Sotomayor, J., concurring).

119. *See id.* at 422 (Alito, J., concurring).

120. *See id.* ("[T]he search of one's home or office no longer requires physical entry, for science has brought forth far more effective devices for the invasion of a person's privacy than the direct and obvious methods of oppression which were detested by our forebears and which inspired the Fourth Amendment." (quoting Goldman v. United States, 316 U.S. 129, 139 (1942) (Murphy, J., dissenting))).

121. *See id.* at 414 (Sotomayor, J., concurring).

Carpenter.[122] The Supreme Court further expanded Fourth Amendment rights in the case of *Carpenter*.[123] Carpenter was prosecuted for multiple counts of robbery and for carrying a gun during a federal crime of violence.[124] The government wanted to use cell-site location information ("CSLI")[125] from Carpenter's cellphone as evidence in the case against him, and the Supreme Court ruled that the government could not use this information.[126] The Court reemphasized that "property rights are not the sole measure of Fourth Amendment violations" and the Court went even further by stating that "the Fourth Amendment protects people, not places."[127] This ruling is significant as it is the first time that the Supreme Court recognized a right to privacy in one's CSLI data.[128]

The Supreme Court's ruling in *Carpenter* vastly expands the reach of Fourth Amendment protections against the government, as now there is a reasonable expectation of privacy in one's cellphone location data.[129] Not only does the Court protect cellphone location data against unreasonable search and seizure under the Fourth Amendment, but the Court also hinted that it might expand these rights into other areas of cybersecurity and data privacy.[130]

The Court has determined that in order for something to be classified as a government seizure and afford Fourth Amendment protection, there must be government interference of a person's freedom of movement or of their possession of their "houses, papers, and effects."[131] The Court has also defined a search as an infringement on "an expectation of privacy that society is prepared to consider

122. Carpenter v. United States, 138 S. Ct. 2206, 2206 (2018); *see infra* Part III.C.

123. *Carpenter*, 138 S. Ct. at 2206.

124. *Id.* at 2212.

125. *Id.*; *Cell Phone Location Tracking*, BERKLEY L., https://www.law.berkeley.edu/wp-content/uploads/2015/04/2016-06-07_Cell-Tracking-Primer_Final.pdf (last visited Apr. 1, 2021) (explaining that cell phone location data is gathered by using the last known location of a cell phone through triangulation). Triangulation is the process of determining the location of a cell phone by using the closest three cell phone towers and their last pings from the cell phone. *Id.* Each of the cell towers then sends the location of the user and is accurate within feet of the cell phone's actual location. *Id.* This data can be very powerful in the hands of a prosecutor, as it can show where a particular defendant or witness was at the time of the event, thereby building up or destroying alibis of those witnesses and defendants. *See id.*

126. *Carpenter*, 138 S. Ct. at 2214, 2222. The "[g]overnment will generally need a warrant to access" cell-site location information ("CSLI") except under certain circumstances where "case-specific exceptions may support a warrantless search of an individual's cell-site records." *Id.* at 2222.

127. *Id.* at 2213.

128. *Id.* at 2214-15.

129. *See id.* at 2219.

130. *See id.* at 2218.

131. Maryland v. Macon, 472 U.S. 463, 469 (1985); U.S. CONST. amend. IV.

reasonable."[132] If the government obtains personal information about an individual through smart speaker data, then it would likely be classified as both a search and a seizure: the government would be interfering with a person's freedom of possession of his or her own data—a seizure—and violating an individual's reasonable expectation of privacy in one's own home—a search.[133]

While the Court in *Carpenter* vastly expanded the reach of the Fourth Amendment and its protections, some circuits have since curbed some of its efficacy through other rulings.[134] In the case of *United States v. Morel*,[135] decided by the First Circuit in 2019, the court ruled that when third-parties can freely access the information being sought by the government, there is no protection under the Fourth Amendment.[136] Although *Morel* strengthens the third-party doctrine within the First Circuit, *Carpenter* still provides a broader reach for the Fourth Amendment's right to privacy, and with it, the possibility that it can be expanded to have an even broader reach upon all circuits.[137]

D. Why Have Federal Legislative and State-Led Efforts Fallen Short?

This Subpart will discuss why recent efforts by state legislators to regulate cybersecurity and privacy concerns do not adequately cover smart speakers.[138] While some states have passed regulations concerning cybersecurity and privacy concerns, the regulations vary in scope and efficacy.[139] For instance, California recently became the first state to pass comprehensive privacy and cybersecurity laws that force companies to tell consumers what information is being gathered and limits how

132. *Macon*, 472 U.S. at 469.

133. *See id.*

134. *See* United States v. Morel, 922 F.3d 1, 8 (1st Cir. 2019) (applying the third-party doctrine, which states that "a person has no legitimate expectation of privacy in information [that one] voluntarily turns over to third parties," since *Carpenter* did not "announce a wholesale abandonment of [it]"); *see supra* notes 125-32 and accompanying text.

135. 922 F.3d 1 (1st Cir. 2019).

136. *Id.* at 8-9. This can prove to be a problematic ruling as constant data breaches make public the personal information of millions of people each year. Mike Snider, *Your Data Was Probably Stolen in Cyberattack in 2018—And You Should Care*, USA TODAY (Jan. 1, 2019, 3:59 PM), https://www.usatoday.com/story/money/2018/12/28/data-breaches-2018-billions-hit-growing-number-cyberattacks/2413411002. It is difficult to imagine that the court intended to include these "public" records in its holding in *Morel*. *Id.*

137. *See* Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018) (stating that the Court should adopt a rule that "must take account of more sophisticated systems that are already in use or in development").

138. *See infra* Part III.D.

139. Adams, *supra* note 18.

long that data can be stored.[140] California's new law provides consumers with more rights than ever before in the space of cybersecurity and data privacy protection.[141] For example, consumers in California can now decide whether or not they want companies to be able to sell their own individual data to third-parties.[142]

Nevertheless, people are torn on what the law will actually do and whether or not it will effectively protect consumers' privacy.[143] Although the law took effect on January 1, 2020, it is still yet to be seen if it will have a significant impact on the way large companies treat consumers' private information.[144] Essentially, the law creates an individual right to one's personal data collected by large companies.[145] In simpler terms, it makes the consumer the owner of the data even though the companies are the ones gathering it through apps, or by use of their services.[146] Although the law is seen as a breakthrough on the cybersecurity and privacy concerns front, it still falls short in a number of ways.[147]

While California's new law spans twenty-four pages and has dozens of provisions, the term "smart speaker" is nowhere to be found in the entire law.[148] In an era of the increasing popularity of smart speakers, and increasing government intrusion on individuals' personal data, not discussing either of these topics in the law is a glaring omission.[149] Moreover, not one provision discusses the government's access to data collected by smart devices.[150] Many hail California's new law as a breakthrough in data protection from corporate interference,[151] but the law does nothing to restrain the government from accessing the very

140. *See id.* (explaining California's new cybersecurity law and temporal limits on how long personal data can be kept for before it must be destroyed).

141. *See* Natasha Singer, *What Does California's New Data Privacy Law Mean? Nobody Agrees*, N.Y. TIMES (Dec. 29, 2019), https://www.nytimes.com/2019/12/29/technology/california-privacy-law.html.

142. *Id.*

143. *See id.*

144. *Id.*

145. *Id.*

146. *Id.*

147. *Id.* One of the ways the new law falls short is on guidance. *Id.* There are a number of disagreements as to how companies should be complying with the new law. *Id.*

148. *See generally* A.B. 375, 2017-2018 Reg. Sess. (Cal. 2018) (enacted) (pointing out that smart speakers are not addressed explicitly by the law).

149. *See id.*

150. *Id.* The law passed includes provisions on what companies may do with an individual's personal data and creates restrictions on when that data must be deleted. *Id.* The law includes other provisions that cover what types of information a consumer can request from companies and whether or not those companies have to turn over all of the data collected about that individual. *Id.*

151. Adams, *supra* note 18 (explaining that California's new law represents "a fundamental shift from the reactionary approach to security governance we've followed since the 1980s").

information it is trying to restrict companies from selling to third-parties.[152]

Utah also recently enacted a law specifically designed to protect private electronic information stored with third-parties from collection by law enforcement without a valid warrant.[153] The new law specifically aims to require law enforcement and government officials to have a warrant before they can request or obtain a person's data held via electronic communication or remote computing providers.[154] The law was enacted to further expand on the protections given in the *Carpenter* decision.[155] Using *Carpenter* as a starting point, Utah expanded the notion of privacy in one's individual location data and codified it into law so that government officials in Utah cannot take advantage of this information without a valid warrant granted by a judge.[156] Under the law, not only do government officials in Utah have to get a warrant to be able to gather location data from individuals, but they must also notify the individual within fourteen days of obtaining the information pursuant to the judicially authorized warrant.[157]

Although this statute is a significant advancement in the field of cybersecurity and data privacy as it pertains to interference by Utah State government, it fails to specifically mention smart speakers and the data collected by them.[158] Moreover, the statute still leaves an opening for the government to gain access to information gathered by smart devices without a warrant under a number of exceptions, including when the device is reported stolen and if the "remote computing service

---

152. A.B. 375.

153. *See* UTAH CODE ANN. § 77-23c-102 (LexisNexis 2021).

154. Allen O'Rourke & Ernesto Mendieta, *New Utah Privacy Law Expands Warrant Requirement for Individual's Data Held by Electronic Communications Service Providers*, NAT'L L. REV. (Apr. 12, 2019), https://www.natlawreview.com/article/new-utah-privacy-law-expands-warrant-requirement-individuals-data-held-electronic. The new law was once known as HB 57, the Electronic Information or Data Privacy Act. *Id.*

155. *Id.*

> Following the Chief Justice's hint [in *Carpenter*], Utah enacted the "Electronic Information or Data Privacy Act" that protects electronic data held by a third party from warrantless access by law enforcement. Specifically, subject to a few exceptions, the law imposes a warrant requirement for law enforcement to obtain (i) location information, stored data, or transmitted data of an electronic device[;] or (ii) electronic information or data transmitted by the owner thereof to a remote computing service provider. As used here, the term "electronic information or data" means "information or data including a sign, signal, writing, image, sound, or intelligence of any nature transmitted or stored in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system."

Id.

156. *Id.*

157. *Id.*

158. *See* § 77-23c-102.

provider voluntarily discloses the location information" in certain circumstances.[159] Even though Utah has taken preliminary steps in protecting its citizens from government intrusion into their personal data collected by smart devices through this law, it still leaves sizeable gaps whereby the government may be able to gain access to this information without a warrant.[160]

Furthermore, there are many states that have introduced legislation that has failed to pass in their legislature.[161] New York is one of those states that could not pass legislation due to political pressures and an unwillingness to alienate the business community through stringent regulations on data privacy and cybersecurity concerns.[162] The proposed bill, known as the New York Privacy Act, would have had a strong resemblance to California's consumer privacy law, but the bill included a private cause of action that would have allowed consumers to sue companies when there is a data breach.[163] Much like the California law, the New York bill also did not mention smart speakers or limit the government's access to data collected by smart devices.[164]

The sharp partisan divide within legislatures, as in New York, makes it hard to pass sweeping privacy acts and cybersecurity regulations.[165] However, a decision by the Supreme Court recognizing broader Fourth Amendment protections of data collected by smart speakers could bypass the political obstacles in state legislatures and yield an effective result that protects an individual's right to privacy.[166]

As seen in New York, the business community can also be a roadblock to legislative solutions.[167] Many businesses are opposed to state-by-state regulations because they are costly for companies operating in multiple states to comply with.[168] Not only is the initial

159. *Id.* § 77-23c-102(2)(a).

160. *See id.*; *see also* Holly Davis, *Utah Just Became a Leader in Digital Privacy*, WIRED (Mar. 22, 2019, 8:00 AM), https://www.wired.com/story/utah-digital-privacy-legislation ("Even with these potentially problematic exceptions, the bill is certainly better than no protections at all.").

161. *See* Lucas Ropek, *NY's Data Privacy Bill Failed; Is There Hope Next Session?*, GOV'T TECH. (July 15, 2019), https://www.govtech.com/policy/NYs-Data-Privacy-Bill-Failed-Is-There-Hope-Next-Session.html.

162. *Id.*

163. *Id.*

164. *See id.*; *see also* S. 5642, 2019-2020 Reg. Sess. (N.Y. 2019).

165. Ropek, *supra* note 161 (explaining how New York State Senator Thomas failed to get the bill off the ground because there was no unified coalition of support behind it).

166. *See infra* Part IV; *see also* Ropek, *supra* note 161.

167. Ropek, *supra* note 161.

168. Eric Newcomer, *California's New Privacy Law Creates $55-Billion Gold Rush for Start-Ups*, L.A. TIMES (Jan. 7, 2020, 2:32 PM), https://www.latimes.com/business/technology/story/2020-01-07/ccpa-55-billion-gold-rush-startups

compliance costly, but a patchwork of state regulations also creates inefficiencies in the system, making it almost impossible for any one company to take on by itself.[169] For these reasons, many companies spend vast amounts of resources on lobbying efforts to stop states from passing their own privacy laws and advocate for a national privacy reform as the only means to a legislative solution.[170] For example, tech companies in particular have lobbied against California's new data privacy law that took effect on January 1, 2020.[171] Many of these companies, including Google, Amazon, and Facebook, have called on Congress to pass a national solution so that they would not have to deal with the compliance problems associated with piecemeal legislation around the country and the world.[172] Businesses, especially tech companies, would prefer not to have any data privacy and security regulations at all, but they would much prefer a national approach to streamline the process and to make it easier for each of them to comply with the regulations if such laws are necessary.[173] Nevertheless, the business community must comply with these new regulations or face harsh penalties if they decide not to come into compliance with each law.[174]

While businesses may be against these laws to protect their bottom line, some companies, notably in tech, have shown a willingness to support overarching federal legislation as opposed to individual laws from each of the fifty states.[175] The American business community is aware that legislation regarding data privacy is coming, as foreshadowed by the European Union's 2018 General Data Protection Regulation, also

---

(explaining how the new California privacy law is going to cost companies $55 billion to begin initial compliance).

169. *See id.*

170. Tony Romm, *'There Is Going to be a Fight Here to Weaken It': Inside the Lobbying War over California's Landmark Privacy Law*, WASH. POST (Feb. 8, 2019, 5:20 PM), https://www.washingtonpost.com/technology/2019/02/08/theres-going-be-fight-here-weaken-it-inside-lobbying-war-over-californias-landmark-privacy-law (explaining how businesses have lobbied to change or eliminate California's new privacy law).

171. *See id.*

172. *Id.*

173. *Id.*

174. Megan Henney, *California Rings in 2020 with Landmark Data Privacy Law*, FOX BUS. (Dec. 31, 2019), https://www.foxbusiness.com/money/california-rings-in-2020-with-landmark-data-privacy-law (explaining how companies have thirty days to fix violations of California's new privacy law or face a $7,500 penalty).

175. *Id.* (highlighting how tech companies have petitioned Congress to take the initiative and pass federal legislation on privacy and data protection in order to make it easier for the companies to comply nationwide and around the world).

known as the GDPR.[176] Even though the business community may not have the best intentions for the consumer when asking for national regulations, it makes a compelling point that regulations should be streamlined to provide uniform protection across the country and in order to make it easier for companies to comply with such regulations.[177]

It is also clear among experts that smart speakers pose a particular cybersecurity and data privacy concern—though there is disagreement as to how this issue should be resolved.[178] Some argue that, while past legislative attempts have failed to properly address this issue, a legislative solution is still the best way to secure an individual's right to privacy in data collected by smart speakers.[179] While some may consider a constitutional approach spearheaded by the Supreme Court to be unnecessary, an extension of Fourth Amendment privacy rights by the Court is the best way to ensure that an individual's personal data is being protected against unwarranted government intrusion.[180]

Some argue that the Supreme Court is particularly well-suited to craft an appropriate solution as it is an institution isolated from outside political pressures.[181] Unlike legislatures, which face pressures from constituents, businesses, and other entities, the Court is insulated from any of those pressures and can create a rule that benefits all citizens without fear of backlash from a particular interest group.[182] Legislatures may also be unwilling or unable to pass the appropriate legislation required to keep individuals' personal data out of the hands of the government due to various partisan divides or political pressures.[183] Legislatures may be unwilling to slight certain groups and are often captured by corporate interests, rendering them unable to provide an

176. *Id.*; Danny Palmer, *What Is GDPR? Everything You Need to Know About the New General Data Protection Regulations*, ZDNET (May 17, 2019, 6:33 AM), https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know.

177. Henney, *supra* note 174.

178. Ryan G. Bishop, Note, *The Walls Have Ears . . . And Eyes . . . And Noses: Home Smart Devices and the Fourth Amendment*, 61 ARIZ. L. REV. 667, 697 (2019).

179. *Id.*

180. *Id.* (citing to Justice Alito's view that "the best solution to privacy concerns may be legislative"). However, even in this statement made by Justice Alito, he uses the word "may," and current legislative action has not gone far enough to include privacy concerns from smart speakers, which should prompt swifter action by the Supreme Court. *Id.* Smart speakers have the potential to give an incredibly detailed look into one's life, "detailing everything from how they like their toast to the layout of their home," which requires urgent action to prevent misuse of this information. *Id.* at 671.

181. *See* STEPHEN POWERS & STANLEY ROTHMAN, THE LEAST DANGEROUS BRANCH?: CONSEQUENCES OF JUDICIAL ACTIVISM 4-5 (2002).

182. *Id.*

183. *See, e.g.*, Ropek, *supra* note 161 (explaining how the New York Legislature was unable to garner support for a broad privacy bill).

adequate solution to the problem.[184] Furthermore, Congress has remained silent on the issue, leaving the states to come up with their own patchwork of legislation—agitating the business community and creating short-term solutions to a long-term problem.[185] This creates a need for an institution isolated from political pressures, namely the Supreme Court, to grant certiorari and rule on a case expanding Fourth Amendment protections over an individual's personal data as collected by corporations.[186]

A solution introduced by the Supreme Court would not only be expedient, but better insulated from the politics of the legislative body.[187] It is clear that the problem of cybersecurity and privacy rights in one's personal data is only expanding and not going away as time passes.[188] The Supreme Court has expanded Fourth Amendment protections over time and now, once again, has the opportunity to expand the right to privacy to include an individual's right to their own personal data against unwarranted government interference.[189] The expansion of the Fourth Amendment right to privacy has been especially strong in cases where individuals seek to keep their private information private.[190] Even assuming that a legislature has the political willpower to pass a cybersecurity law that creates a right to privacy in one's personal data collected by smart speakers, a subsequent legislature could decide to strip these regulations at any time.[191] In any given election cycle, a legislature's attitude towards regulating smart speakers may change,

184. *See, e.g.*, *id.* (describing the tech- and business-oriented lobbyists that appeared at the hearings to oppose the New York bill).

185. *See* Henney, *supra* note 174.

186. *See infra* Part IV.

187. *See* POWERS & ROTHMAN, *supra* note 181, at 4-5 (describing the Court as an institution "that is insulated enough from public opinion and political expediency to rule on the basis of principle, constrained by the application to cases and controversies, yet not so constrained as to be prevented from rising above the case and invoking and enforcing general principles").

188. *See* Michael Chertoff & Jeremy Grant, *8 Ways Government Can Improve Their Cybersecurity*, HARV. BUS. REV. (Apr. 25, 2017), https://hbr.org/2017/04/8-ways-governments-can-improve-their-cybersecurity (arguing that governments must implement a more permanent solution to the problem of cybersecurity and privacy concerns).

189. Allen, *supra* note 90, at 180-91 (explaining major Fourth Amendment decisions and their potential implications for smart devices).

190. *See id.* at 183 & n.149.

191. *See* Romm, *supra* note 170. Legislators are faced with various interest groups—including, but not limited to, individual citizens and large corporate lobbyists—and they all have ranging interests in what they want to see included or excluded from privacy regulations. *Id.* A change in public opinion could be the end of the line for a piece of legislation where constituents plea with elected officials to "remember all of us," as legislators make decisions on what provisions will or will not be included. *Id.*

leading that session of the legislature to repeal any laws that may have been passed solving the issue.[192]

The legislative solution does not only fall short in that it can be repealed at any time; it may also fail to provide adequate protection to individuals as various legislators may have competing interests resulting in a final bill that does not adequately remedy the problem.[193] The Supreme Court is supposed to be removed from all of the varying interests that face legislators, such as constituents, donors, and personal obligations.[194] The Court is able to come in and not only identify the exact issue by taking a case on appeal, but it can also prescribe a calculated and effective long-term solution to the problem.[195] As smart speaker popularity continues to grow, with no slowdown in sight, it is important that the solution to warrantless government interference in personal data collected by smart speakers be both effective and able to stand the test of time.[196]

IV. MEANS TO AN END: DECIDING A CASE THAT GRANTS AN EXPANDED FOURTH AMENDMENT RIGHT TO PRIVACY

This Part will explain why the Supreme Court should interpret the Fourth Amendment right to privacy to require the government to obtain a warrant before accessing data collected by smart speakers.[197] Subpart A will go on to lay out how and why the Supreme Court should decide a case that expands upon an individual's Fourth Amendment rights against the government in their personal data collected by smart speakers.[198]

192. *Id.* Explaining how legislators are told that privacy and cybersecurity legislation could be a "third rail," and that they should be "careful [of] what [they] touch, be careful what [they] do, because [they] may get away with something for a while—but if the voters and consumers find out what [they] did, [they] might find [themselves] in trouble." *Id.* This underscores the legislature's sensitivity to the electorate and special interests that influence legislation, illustrating that legislators could repeal or change a law that is presented with fierce backlash or opposition. *Id.*

193. *Id.* (describing, as an example, the competing interests at play in the newly passed California legislation).

194. *See* POWERS & ROTHMAN, *supra* note 181, at 4-5.

195. *Id.* at 3 (describing how the strategic advantages of actions by courts are often underestimated, as modern courts function in a "heavily bureaucratic policy-making environment").

196. *See* Williams, *supra* note 5; *see infra* Part IV.

197. *See infra* Part IV.

198. *See infra* Part IV.A.

A. The Court Needs to Recognize a Fourth Amendment Right to Privacy in Data Collected by Smart Speakers

This Subpart discusses a possible solution to the data privacy issue posed by smart speakers.[199] The solution is for the Supreme Court to decide a future case that will expand upon an individual's Fourth Amendment right to privacy against the government, which in turn will limit the government's access to one's personal data collected by smart speakers.[200] Over time, the Court has expanded the Fourth Amendment right to privacy from a simple right against common-law trespass of property to a broader right of privacy, even when there is no physical intrusion onto one's property.[201] The Court's rulings in *Katz*, *Jones*, and *Carpenter* helped set up a legal framework for the Court to potentially hear a case that would extend Fourth Amendment protection to individuals' personal data collected by smart speakers against warrantless government intrusion.[202] When evaluating Fourth Amendment issues, the Court applies one of two predominant ideologies: the "living Constitution" approach or the textualist/originalist approach.[203]

A traditional approach to analyzing Fourth Amendment issues is to consider the question through the lens of the "living Constitution."[204] In a speech delivered by Supreme Court Justice Thurgood Marshall in 1987 at the Constitution's bicentennial celebration, he argued that the Constitution must be interpreted in light of evolving political, moral, and societal norms in order to best serve the people in the modern era.[205] Justice Marshall was one of many Supreme Court Justices that has advocated for a living, breathing Constitution that evolves with the times and helps the Court to craft modern solutions for modern problems.[206] Justice Stephen Breyer is another Justice that has called for a living Constitution approach that can evolve through application with changing

199. *See infra* Part IV.A.

200. *See infra* Part IV.A.

201. Kerr, *supra* note 99, at 802; United States v. Jones, 565 U.S. 400, 414 (2012) (Sotomayor, J., concurring).

202. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); *Jones*, 565 U.S. at 414 (Sotomayor, J., concurring); Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018).

203. Stuart Taylor Jr., *Marshall Sounds Critical Note on Bicentennial*, N.Y. TIMES (May 7, 1987), https://www.nytimes.com/1987/05/07/us/marshall-sounds-critical-note-on-bicentennial.html; *see* Andrea Seabrook, *Justices Get Candid About the Constitution*, NPR (Oct. 9, 2011, 12:58 AM), https://www.npr.org/2011/10/09/141188564/a-matter-of-interpretation-justices-open-up.

204. Taylor Jr., *supra* note 203.

205. *See id.*

206. *Id.* While Justice Marshall was critical of the way much of the Court had decided previous cases, he made a strong point that the Court should look at the Constitution as a living, breathing document that can adapt to the times. *Id.*

societal values and norms.[207] Justice Breyer has said that "[t]rying to apply this Constitution—with those values underlying the words—to circumstances that are continuously changing is not something that can be done by a computer."[208] Justices that believe in a living Constitution call for the Court to make value decisions, rather than only analyze the text, when solving the legal questions presented.[209]

The Court employed the living Constitution approach in *Katz*.[210] Justice Harlan's two-prong test in *Katz* was designed to adapt and reflect what "the majority of society was prepared to hold as a reasonable expectation of privacy."[211] The Supreme Court continues to use and mention the living Constitution methodology from *Katz* when deciding questions of Fourth Amendment rights to privacy.[212] In applying this test to the issue at hand pertaining to smart speakers, the Court should conclude that there is a reasonable expectation of privacy in one's personal data collected by smart speakers, and that Fourth Amendment protections should be extended, because: (1) most individuals would subjectively believe that the conversations they have in the privacy of their own homes remains private and outside of the reach of the federal government through recordings on a smart speaker; and (2) that expectation of privacy is deemed reasonable by society as the Court has already ruled in the past that society expects and deserves the greatest amount of privacy in one's home.[213]

Furthermore, the Supreme Court's decision in *Carpenter* also lends support to this argument.[214] The Court stated that "the retrospective quality of the data here gives police access to a category of information otherwise unknowable."[215] Not only does this rationale leave an open-ended limit on the government from obtaining information from devices that provide data of a "retrospective" nature, but this vague language also invites the Court to revisit other technologies that raise

207. Seabrook, *supra* note 203.

208. *Id.*

209. *Id.*

210. *See* Katz v. United States, 389 U.S. 347, 361 (1967).

211. Navid Massarat, *Living or Dead: Privacy Rights in the Digital Age*, GEO. WASH. JUST. J. (Nov. 28, 2020), https://gwjusticejournal.com/2020/11/28/living-or-dead-privacy-rights-in-the-digital-age.

212. *See id.* However, it must be noted that in more recent cases, the Court has not strictly adhered to the traditional logic of *Katz*, but has nonetheless used it as a significant basis for its decisions. *See id.*

213. *See Katz*, 389 U.S. at 361 (Harlan, J., concurring).

214. *Carpenter*, 138 S. Ct. at 2213.

215. *Id.* at 2218.

similar concerns.[216] Moreover, the language that the Court uses could support a similar ruling pertaining to smart speakers.[217]

Similar to cellphone location data, data collected by smart speakers is retrospective and gives an exact recount of what an individual said at a time where the individual felt that they had the most privacy: in their own home.[218] Additionally, the information collected by smart speakers is also otherwise unknowable, as individuals are presumed to have the highest level of privacy in their own homes,[219] and since smart speakers are often found within the home, they should be considered outside of the reach of warrantless government intrusion.[220] The Court in *Carpenter* provided strong precedent for extending the Fourth Amendment right to privacy to cover data collected by smart speakers using the living Constitution methodology.[221]

Nevertheless, those opposed to extending Fourth Amendment privacy rights to data collected by smart speakers may be quick to point to the third-party doctrine.[222] They would argue that individuals who use smart speakers have to agree to the terms and conditions in the user agreement, which allows the tech companies to use the data collected for marketing purposes or to sell the information to third parties.[223] They would further argue that this third-party disclosure effectively puts users on notice, eliminating any expectation of privacy even if the device is found in one's home.[224] Detractors may also cite *Katz*, where the Court held that those who knowingly expose their personal information to the public, even in their own home or office, are not subject to Fourth Amendment protections.[225]

However, there may be issues with this reasoning as many users do not read the terms and conditions before accepting them, which defeats

---

216. *Id.*

217. *Id.* (explaining how the Court "must take account of more sophisticated systems that are already in use or in development"). Here, it can be argued that smart speakers are the very kind of technology that the Court says it must "take account of" to provide greater Fourth Amendment protections in the modern era. *Id.*

218. *See id.* (discussing how retrospective CSLI data can be used to retrace an individual's entire schedule and movement history).

219. *See id.*; Kerr, *supra* note 99, at 810-11 (explaining that the Court has consistently held that individuals' rights to privacy are greatest in their homes).

220. *See* Allen, *supra* note 90, at 184-85; Kerr, *supra* note 99, at 811.

221. *See Carpenter*, 138 S. Ct. at 2213.

222. *See* Allen, *supra* note 90, at 168-69. The third-party doctrine means that "[a] person has no legitimate expectation of privacy in information [they] voluntarily turn[] over to third parties." Smith v. Maryland, 442 U.S. 735, 743-44 (1979).

223. Allen, *supra* note 90, at 182-83.

224. *Id.* at 177.

225. Katz v. United States, 389 U.S. 347, 351-52 (1967).

the knowledge requirement.[226] Moreover, even if the Court were to rule that *not* having read the terms and conditions cannot defeat the knowledge standard of exposing personal information to the public, the Supreme Court should still extend Fourth Amendment protection to data collected by smart speakers because, as the Court itself said in *Katz*, "what [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[227] This is especially true when most consumers, although voluntarily using smart speakers, are not aware of the full extent to which data can be stored and used.[228]

Furthermore, the Court in *Carpenter* examined the third-party doctrine issue and largely dismissed any questions surrounding whether access by a third party would defeat Fourth Amendment protection.[229] The Court recognized that by using a cellphone, individuals give a third party access to their data; however, it swept away any concerns regarding the third-party doctrine.[230] The Court ruled that "the fact that the Government obtained the information from a third party does not overcome Carpenter's claim to Fourth Amendment protection."[231] The Court made it clear that the fact that a third party may have access to an individual's cellphone location data does not preclude Fourth Amendment protections.[232]

This is significant because the *Carpenter* Court was willing to extend Fourth Amendment protections over cellphone location data by minimizing the importance of the third-party doctrine.[233] The case for smart speakers is even stronger than the case presented in *Carpenter*, as the data being recorded is more personal than one's cellphone location data.[234] Such data would potentially give the government access to actual

226. Allen, *supra* note 90, at 182 & n.143 (explaining how few users actually read all of the terms and conditions of the items they buy and, instead, simply begin using them). Many of the users are actually unaware of what policies they agree to but neglect the terms and conditions document because its length and usage of vernacular that an average individual cannot clearly understand. *Id.*

227. *See Katz*, 389 U.S. at 351.

228. *See* Timm, *supra* note 15 (explaining that "[w]hile people voluntarily use all these devices, the chances are close to zero that they fully understand that a lot of their data is being sent back to various companies to be stored on servers that can either be accessed by governments or hackers").

229. 138 S. Ct. 2206, 2220 (2018).

230. *Id.*

231. *Id.*

232. *See id.*

233. *Id.*

234. *See* Bishop, *supra* note 178, at 679-80. Data recorded by smart speakers is vast and can range from access to videos or a user's media library, to text messages, to information about one's home, ranging from the temperature, to the lighting, or even a user's credit card information, as well

recordings of conversations from an individual's home.[235] The Court has shown that the third-party doctrine must cede to Fourth Amendment protections when sensitive personal data is involved, and, here, it is unquestionable that the data collected is even more sensitive data than that in *Carpenter*, where the Court nonetheless decided to extend Fourth Amendment protections.[236] Nevertheless, the dissent in *Carpenter* highlights the textualist argument surrounding the Fourth Amendment analysis which must also be examined.[237]

Textualists and originalists have had a profound influence on the Court, and it is important to analyze their methodology of deciding whether or not they would expand Fourth Amendment privacy rights to one's personal data collected by smart speakers.[238] From Justices Scalia and Thomas, to the recently appointed Justices Gorsuch, Kavanaugh, and Barrett, it seems likely that some Justices on the Court will employ textualism and originalism when deciding upcoming cases on the docket.[239] Originalists and textualists adhere strictly to what the framers had intentioned at the founding of the country and what the words in the Constitutional themselves mean, without allowing for interpretive changes to the document's meaning in line with the times.[240]

Traditionally, originalists emphasize common law trespass when examining questions of Fourth Amendment rights to privacy, with a focus on physical intrusion.[241] In the case of *Kyllo v. United States*,[242] a Scalia opinion, the Court made it clear that any government intrusion into an individual's home is presumptively unreasonable without a warrant.[243] The Court in *Kyllo* highlighted that "any physical invasion of

---

as a whole host of information that the user decides to store on their devices and make accessible to a smart speaker via the IoT. *Id.*

235. *See* Schirm, *supra* note 18.

236. 138 S. Ct. at 2220.

237. *Id.* at 2224 (Kennedy, J., dissenting).

238. John Greabe, *Constitutional Connections: Textualism and Originalism in Constitutional Interpretation*, CONCORD MONITOR (Feb. 12, 2017, 12:20 AM), https://www.concordmonitor.com/Textualism-and-originalism-in-constitutional-interpretation-8000920; *see generally, e.g.*, Max Alderman & Duncan Pickard, *Justice Scalia's Heir Apparent?: Judge Gorsuch's Approach to Textualism and Originalism*, 69 STAN. L. REV. ONLINE 185 (2017) (explaining the effect that Justice Scalia has had on the Court in recent years and his use of originalism and textualism when deciding cases before the Supreme Court).

239. *See* Noah Feldman, *The Battle over Scalia's Legacy*, N.Y. REV. (Dec. 17, 2020), https://www.nybooks.com/articles/2020/12/17/the-battle-over-scalias-legacy.

240. *See* Seabrook, *supra* note 203 (explaining how Justice Scalia, in particular, strictly adhered to originalism during his time on the Court and how he made sure that he did not stray from the original meaning of the text of the Constitution in his decisions).

241. *See* William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 HARV. L. REV. 1821, 1834, 1840 n.101 (2016).

242. 533 U.S. 27 (2001).

243. *Id.* at 40.

the structure of the home 'by even a fraction of an inch,' was too much . . . . In the home, our cases show, *all* details are intimate details, because the entire area is held safe from prying government eyes."[244] This case shows how the Supreme Court holds dear the right to privacy in one's own home, especially in the case of actual, physical intrusion.[245]

In applying the originalist approach to determine whether or not the Court should extend the Fourth Amendment right to privacy to protect an individual's personal data collected by smart speakers, it is important to note that there is no physical intrusion into the home with smart speakers.[246] While smart speakers do not pose the issue of traditional common law trespass, involving government entrance into a private home, they pose a strikingly similar threat by giving the government access to what an individual does in their own home *even without* the physical intrusion.[247] Justices that subscribe to the originalist methodology, and are concerned with governmental physical trespass into the home,[248] would likewise be alarmed by the information collected by smart speakers in the privacy of one's home.[249]

Not only do individuals expect a right to privacy in their own home, but the Supreme Court has also traditionally held that one's home is outside the reach of warrantless government intrusion.[250] Accordingly, originalist Justices may also vote to extend the right to privacy in one's

244. *Id.* at 37.

245. *See id.*

246. Allen, *supra* note 90, at 181.

247. *See id.* at 184-85.

248. *See generally* Carpenter v. United States, 138 S. Ct. 2206, 2272 (2018) (Gorsuch, J., dissenting) (explaining how Justice Gorsuch believes it was a mistake that the Court did not analyze the issue presented using a "more traditional approach").

249. *Id.* While Justice Gorsuch dissented in *Carpenter*, he makes it clear that he would have been more inclined to extend Fourth Amendment protections had the majority engaged in a "more traditional approach" to the issue. *Id.* Justice Gorsuch goes as far to say, "I cannot help but conclude—reluctantly—that Mr. Carpenter forfeited perhaps his most promising line of argument" by not arguing "the law of property or any analogies to the common law." *Id.* Justice Gorsuch makes it clear that he is "reluctantly" in the dissent because Mr. Carpenter failed to approach the issue in a way that would be more appealing to traditional textualist/originalist justices. *Id.* Justice Gorsuch even tees up the argument for a future case, saying, "Plainly, customers have substantial legal interests in this [CSLI collected by smartphones], including at least some right to include, exclude, and control its use." *Id.* Justice Gorsuch goes even further to suggest that "[t]hose interests might even rise to the level of a property right." *Id.* This language is strong, and goes to show that even textualist/originalist Justices, such as Justice Gorsuch, see the need to extend Fourth Amendment protection to modern devices that reveal the intimate details of individuals. *Id.* Justice Gorsuch's willingness to extend the Fourth Amendment's traditional property right to CSLI bodes well, as it pertains to his willingness to extend protection to data collected by devices like smart speakers, which are even more revealing and found within one's home. *Id.*

250. Allen, *supra* note 90, at 167. The Supreme Court has held time and time again that an individual's home is held in high regard, and the Supreme Court continues to find that any warrantless government intrusion into the home must meet a high bar. *Id.*

home, as it is more important than ever, in our increasingly globalized and interconnected world, that individuals' intimate and private details and conversations are kept from warrantless government intrusion.[251] Once again, while there is no physical trespass, there is, in fact, access to an individual's home, as smart speakers can and do record the intimate conversations that individuals have in their bedrooms, kitchens, and living rooms.[252] The government currently faces no bar in obtaining this information from the tech companies themselves, and if the government gets ahold of this information, it would be able to get a detailed look into one's life, which is analogous, if not more expansive, than the information the government would gather from physical intrusion into an individual's home.[253] This would likely alarm originalist Justices, leading them to also vote to expand the Fourth Amendment right to privacy to include data collected by smart speakers.[254]

The Supreme Court has emphasized that privacy is greatest in one's own home, and since smart speakers are generally found in the home, the Justices would likely find that they are subject to Fourth Amendment protection from the government.[255] Moreover, consumers who have smart speakers in their homes do not change their actions because of this new piece of technology, perhaps because they are unaware of its power; however, that device can provide data to the government, which the government can try to use against them in a potential criminal or civil proceeding.[256] The government should not be able to intrude, via smart speakers, into one's home without a valid, court-ordered warrant.[257] As Justices Alito and Sotomayor noted in *Jones*, it does not matter that the government is not physically intruding into an individual's home; technology is giving the government more direct access and this, too, should be barred by the Fourth Amendment right to privacy.[258]

Further applying the originalist view in attempting to determine what the founding fathers would think about this issue would be a difficult task, but it is likely that they would not be happy with the

251. *See id.* at 171 (explaining an originalist view taken by the Court, holding that "[a]t the very core of the Federal Constitution's Fourth Amendment stands one's right to retreat into one's home and there be free from unreasonable government intrusion" (quoting Kyllo v. United States, 533 U.S. 27, 31 (2001))).

252. *See id.* at 181.

253. *See* Schirm, *supra* note 18.

254. *See supra* note 248 and accompanying text.

255. Kerr, *supra* note 99, at 811.

256. *See, e.g.*, McLaughlin, *supra* note 60.

257. *See* United States v. Jones, 565 U.S. 400, 405 (2012) (discussing how one's home is sacred and should be free from intrusion via the Fourth Amendment's right to privacy).

258. *Id.* at 414 (Sotomayor, J., concurring); *id.* at 426-29 (Alito, J., concurring).

government's warrantless access to information collected by a device within a person's home.[259] The founding fathers were adamant about protection from government interference in one's personal life, which is precisely why they adopted the Fourth Amendment after the ratification of the Constitution.[260]

The Fourth Amendment sheds light on the founding fathers' intent to protect a person's home from unreasonable searches and seizures, and it is not unreasonable to believe that the founders would find that a smart speaker's recording capabilities, and the data that they collect, should be protected from unreasonable search and seizure by the government.[261] This new technology provides an avenue for the government to intrude into the home—a space that originalists adamantly apply Fourth Amendment protections—which would allow warrantless government intrusion into the most intimate details of an individual's life.[262] For the aforementioned reasons, if the Court chooses to apply the textualist or originalist approach, the Court would still be able to decide a case expanding Fourth Amendment protections over data collected by smart speakers, while staying true to its methodology of deciding cases.[263]

While the Court has a variety of Justices who subscribe to both the originalist/textualist methodology, as well as the living Constitution methodology, the Court can and should extend the Fourth Amendment right to privacy from prying government eyes to cover personal data obtained from smart speakers.[264] Either aforementioned method of reasoning can be used to arrive at the same conclusion.[265]

There are also a number of policy reasons as to why the Supreme Court should decide a case that expands the Fourth Amendment right to privacy over one's personal data collected by smart speakers.[266] Without the Supreme Court's interference, it is likely that Congress will continue to drag its feet and take no action in the area of smart speaker privacy and cybersecurity concerns.[267] It is also likely that if the Court takes no

259. *See* Brian Frazelle & David Gray, *What the Founders Would Say About Cellphone Surveillance*, ACLU (Nov. 17, 2017, 1:45 PM), https://www.aclu.org/blog/privacy-technology/location-tracking/what-founders-would-say-about-cellphone-surveillance (describing what the founding fathers would likely think about large tech companies giving the government access to gather surveillance intelligence from a person's cellphone data).

260. *Id.*

261. *See* Frazelle & Gray, *supra* note 259.

262. *See supra* Part IV.A.

263. *See supra* Part IV.A.

264. *See supra* Part IV.

265. *See supra* Part IV.

266. *See supra* Part IV.

267. Romm, *supra* note 170. Every year technology companies spend vast amounts of resources trying to lobby Congress to come up with a permanent national solution to cybersecurity

action, individual states will continue to come up with their own legislative solutions that will be ineffective and create hurdles in businesses' compliance.[268] Furthermore, without any intervention, consumers will continue to buy smart speakers, without knowing of the extent of the risks that come with them, which only exacerbates the problem by putting more smart speakers in the homes of Americans without any adequate protection for their data and privacy.[269] If the Court does not take action, there will be no winners, as Congress will likely fail to appropriate action; state legislatures will likely not be able to create a patchwork of laws that adequately protect consumers; technology companies will have to comply with a variety of laws passed by the states; and consumers will continue to buy smart speakers, which increases the risk of government abuse without any adequate privacy safeguards.[270]

V. CONCLUSION

Smart speakers are an increasingly popular technological item that are often found within the homes of many Americans.[271] While smart speakers can make life more convenient, they do so by intruding and listening in on personal conversations held by individuals in their own homes.[272] Smart speakers can and do record the intimate conversations of Americans in their own homes.[273] Although this technology is relatively new, it is alarming that there are no federal regulations as to the use of the data collected by smart speakers or as to whom the data can be given.[274] This lack of regulation and protection against government intrusion creates an urgent problem—one which the Court has the ability to solve.[275]

If the Supreme Court hears a case on smart speakers, and subsequently extends Fourth Amendment privacy protections to data collected by smart speakers, immediate cybersecurity and privacy

---

and privacy concerns surrounding smart speakers. *Id.* Every year that Congress fails to take action on a national level causes these companies to spend more and more in compliance costs, trying to ensure that they are able to comply with the patchwork of new state laws that crop up. *Id.*

268. *See id.*

269. *See* Ingersoll, *supra* note 12 (describing how consumers are aware of certain data privacy risks when purchasing a smart speaker, yet they are continuing to buy them at record rates).

270. *See supra* Part IV.

271. Williams, *supra* note 5.

272. *See How Creepy Is Your Smart Speaker?*, *supra* note 7.

273. *See* Bishop, *supra* note 178, at 688.

274. Schirm, *supra* note 18.

275. *See id.*

concerns surrounding these devices would be greatly alleviated.[276] The Supreme Court is the proper place to address the issue of smart speaker privacy rights against government intrusion because the Court has the power to do so by simply extending the Fourth Amendment right to privacy against government intrusion to cover smart speakers.[277] The Court can also circumvent the political process and Congress, which, to date, has avoided taking any stance on the issue.[278] Additionally, the Court can provide much-needed protections to the consumers who continue to purchase smart speakers—both those who are fully aware of the cybersecurity and privacy issues that come along with the device and those who are not.[279] For all of these reasons, the Supreme Court not only has the power to address the issue of smart speaker privacy rights against government intrusion, but it also should exercise this right.[280]

*Jacob A. Manzoor**

276. *See supra* Part IV.
277. *See supra* Part IV.
278. *See supra* Part III.D.
279. Ingersoll, *supra* note 12.
280. *See supra* Part IV.

* J.D. Candidate, 2021, Maurice A. Deane School of Law at Hofstra University; B.A., Political Science, *magna cum laude*, 2019, Hofstra University. I would like to thank my family for their love and support throughout law school and for their encouragement throughout the entire publication process. I would also like to thank my Faculty Advisor, Professor Matthew Shapiro, for his help and support throughout the writing process, and for his intellect and insight on this topic and others. Finally, I would like to thank all members of Volume 49 and Volume 50 of the *Hofstra Law Review*, with special gratitude to the Managing Editors, Leanne Bernhard, Delores Chichi, and Robert Levinson; Articles Editor, Matthew Hauszpigel; Research Editor, Daniel Axelrod; and Notes Editor, Alexandra Piscitello.

***