PRIVACY IN THE TWENTY-FIRST CENTURY SMART HOME

Susan Allen[1]

I. Introduction

It was not long ago that Apple released its Siri feature wowing consumers with both its capabilities and cutting-edge technology.[2] Suddenly the term "smart phone" took on a whole new meaning with Siri's ability to text, call, find directions, and do much more.[3] To some, it only seems natural that the next development will be that of the "smart home."[4] Enter the Amazon Echo, first released in 2014.[5] Originally perceived as a smart speaker, the Echo and its Alexa personification have the ability to carry out over 500 tasks, all initiated simply through the utterance of a "wake word."[6] For example, an Echo

---

[1]Susan Allen, J.D. Candidate, Suffolk University Law School, 2019.
(This piece differs from the March 2018 University of Washington Law Review article because it focuses on history of the Fourth Amendment and related case law. It also makes a prediction on how courts will rule on relevant cases in future litigation and does not address the technology behind the Alexa product or the current legislation existing today.)

[2] *See* Luke Dormehl, *Today in Apple History: Siri Debuts on iPhone 4s*, CULT OF MAC (Oct. 4, 2017), *archived at* https://perma.cc/E4YE-7QU5 (reporting on the seven-year anniversary of Apple's Siri feature).

[3] *See id.* (describing the exciting new features exhibited at the time of Siri's release).

[4] *See If These Walls Could Talk: The Smart Home and the Fourth Amendment Limits of the Third Party Doctrine*, 130 HARV. L. REV. 1924, 1939 (2017) (explaining that recent developments in technology are redefining the home and that the widespread development of "smart homes" is likely to occur in the near future); s*ee also* Julianne Pepitone, *Google House: Tech Giant Spends Billions to Get Inside Your Home*, CNBC (Jan. 15, 2014), *archived at* https://perma.cc/W8FX-22QW (reporting on Google's $3.2 billion purchase of Nest Labs, the producer of a sci-fi smart thermostat); *see also* Andreas Jacobsson, *On Privacy and Security in Smart Homes*, MEDIUM.COM (June 13, 2016), *archived at* https://perma.cc/A9BC-B8U3 (exploring the concept of smart homes as a growing phenomenon in modern life).

owner can inquire about the weather or the score of a recent sports event by merely wondering out loud.[7] Some perceive this impressive development of technology as threatening, fearing that artificial intelligence will someday overtake humankind; however, most purchasers remain simply amazed by the Echo's capabilities.[8]

Nevertheless, the Echo's tremendous ability carries with it a slew of legal questions. Much like its competitors, such as Apple's Siri or Microsoft's Cortana, the Echo collects and stores all of a user's inquiries, as well as any inadvertent comments made after the device's activation.[9] This understandably distresses consumers, however, companies such as Amazon maintain that their privacy policies provide users with the requisite notice that their data is to be collected.[10] Furthermore, this practice now raises concern as to what

[5] *See* Matt Weinberger, *How Amazon's Echo Went from a Smart Speaker to the Center of Your Home*, BUS. INSIDER (May 23, 2017), *archived at* https://perma.cc/HGX7-KSXM (identifying when Amazon first introduced the Echo); *see also* Kim Wetzel, *What is Alexa? It's Amazon's Virtual Voice Assistant*, DIGITALTRENDS (May 11, 2018), *archived at* https://perma.cc/6KV4-XE5B (introducing Alexa as a virtual assistant integrated into several of Amazon's products, including the Echo). "Alexa can perform a variety of simple tasks, like playing music, but it can also be used to control smart-home gadgets, giving it the ability to dim the lights, lock the doors, or adjust the thermostat." *Id.*

[6] *See id*. (discussing how early critics of the Echo regarded it as little more than an advanced speaker system for playing music, although it now can complete over 500 tasks).

[7] *See id.* (providing examples of the numerous tasks the Echo can perform).

[8] *See* Rory Carroll, *Goodbye Privacy, hello 'Alexa': Amazon Echo, The Home Robot Who Hears It All*, THE GUARDIAN (Nov. 21, 2015), *archived at* https://perma.cc/Z8X5-KCN5 (pointing out examples of mixed responses to the Echo's advanced abilities); *see also* John Chambers, *Are You Ready for the Internet of Everything?*, WORLD ECONOMIC FORUM (Jan. 15, 2014), *archived at* https://perma.cc/S7BD-69W3 (concluding that the expansion of the Internet of Things is "changing *everything* and as a result, everyone will benefit").

[9] See Carroll, *supra* note 8 (describing how it is a standard procedure for smart devices to collect data and send it to the cloud).

[10] *See* Alex. B. Lipton, *Privacy Protections for Secondary Users of Communications-Capturing Technologies*, 91 N. Y. U. L. REV. 396, 413 (2016) (referencing that the existence of policy agreements results in consumers neither reading nor understanding them).

happens to such data after its collection, and for what purposes it may be utilized.[11] Aside from the commercial use of data collected from within the home, there now exists a new method for the government to infiltrate the homes and private lives of American citizens.[12] Consumers are alarmed by the government's new ability to monitor daily life because of the intimate nature of the home setting.[13] This is especially noteworthy when one considers that for nearly two hundred years after the nation's founding, the government could not obtain private papers as evidence of criminal activity, regardless of the existence of a warrant.[14] While we cannot be certain of what developments lay ahead, we can anticipate possible complications arising from new technological advances by examining the past.

II. History

The Framers of the United States Constitution included the Fourth Amendment to protect United States citizens against unreasonable searches and seizures.[15]

---

[11] *See id.* at 413 (questioning the purpose of collecting Echo user's data and what happens to it after it goes to the cloud); *see also* Nicole Perlroth and Nick Bilton, *Mobile Apps Take Data Without Permission*, N.Y. TIMES (Feb. 15, 2012), *archived at* https://perma.cc/63VW-KMRY (demonstrating that the fact that mobile device applications kept user information was shocking news in 2012).

[12] *See* Pelroth and Bilton, *supra* note 11 (detailing how authorities sought data from the Echo of a murder suspect).

[13] *See* Tony Bradley, *How Amazon Echo Users Can Control Privacy*, FORBES (Jan. 5, 2017) *archived at* https://perma.cc/34TH-EEKP (suggesting methods to alter the Echo's privacy settings); *see also* Amazon Help & Customer Service, *Alexa Terms of Use*, AMAZON (2017), *archived at* https://perma.cc/6UDR-ZNHR (listing Amazon's user agreement and terms of use for the Echo and its Alexa feature).

[14] *See* James B. Comey, Dir. Fed. Bureau of Investigation, *Exceptions of Privacy: Balancing Liberty, Security, and Public Safety*, Remarks to the Center for the Study of American Democracy Biennial Conference at Kenyon College, at 2-3 (Apr. 6, 2016), *archived at* https://perma.cc/F86X-M675 (providing a brief glimpse into the history of the government's ability to search and seize items from citizens).

[15] *See* Barry Friedman & Orin Kerr, *Common Interpretation: The Fourth Amendment*, CONSTITUTION CENTER (Oct. 19, 2017), *archived at* https://perma.cc/23MX-VTRU (explaining the ratification of the Fourth Amendment in relation to Constitution).

In the decades leading up to the framing of the Constitution, the New World colonists lived under the rule of the British Crown.[16] The British Crown employed general warrants and writs of assistance as measures to combat political opposition and the possession of untaxed consumer goods such as salt, sugar, and foreign imports.[17] The colonists were concerned about the seemingly endless and limitless searches ordered by the crown because of early notions that a man's home was his castle.[18] James Otis stated, "One of the most essential branches of English liberty is the freedom of one's house. A man's house is his castle; and whilst he is quiet, he is well guarded as a prince in his castle."[19] Although they ultimately rejected rule under the crown, the colonists remained inspired not by what the Magna Carta said, but instead what it had come to mean.[20] William Pitt demonstrated the meaning of the Magna Carta when he addressed Parliament in 1763 and declared:

> The poorest man may, in his cottage, bid defiance to all the forces of the Crown. It may be frail; its roof may shake; the wind may blow through it; the storm may enter, the rain may

[16] *See id.* (reminding readers of the political landscape that existed during the early days of the thirteen colonies).

[17] *See id.* (setting forth the British crown's purpose and use of general warrants and writs of assistance in the colonial period).

[18] *See* Leonard W. Levy, *Origins of the Fourth Amendment*, 114 ACAD. OF POL. SCI. 79, 79 (1999) (articulating that the notion that one's home was also his castle originated long before the Bill of Rights and the Fourth Amendment).

[19] *See* Brief for Plaintiffs, *Paxton's Case*, Mass. Sup Ct. 24-26 (1761) [hereinafter *Paxton's Case*] (providing evidence of the notion that a man's home was his castle even before the emergence of the Fourth Amendment, as is clear in pre-American Revolution case law); *see also* James Otis, *Against Writs of Assistance* (Feb. 24, 1761), *archived at* https://perma.cc/3ZN8-E8R3 (arguing against the legality of Britain's general writs of assistance in favor of narrower methods for conducting searches and seizures).

[20] *See* Otis, *supra* note 19 (detailing that although the colonists resisted much of the British rule over them, the Magna Carta remained an influential document in political mindsets).

> enter, but the King of England may not enter; all his force dares not cross the threshold of the ruined tenement.[21]

Thus, concern existed regarding the sanctity of the home decades before the framing of the Constitution.[22] Nonetheless, as colonists began to feel more and more oppressed by the British crown, they sought to create their own laws and governments.[23] Instead of referring to British law as a precedent for the colonies, the would-be framers instead repudiated it and set out to create new laws.[24] One of their major objectives was to end the pervasive use of general warrants and writs of assistance.[25] In 1756, the then province of Massachusetts did just this and "abandon[ed] general warrants in favor of warrants founded on some elements of particularity."[26] Other colonies would follow this trend and incorporate similar law in their respective Declaration of Rights.[27] Finally, after much conflict about the specific wording of the clause, the Framers included the Fourth Amendment in the Bill of Rights in 1791.[28]

A. The Scope of the Fourth Amendment

The law and modern technology have seemingly always conflicted with one another. Not only is this true today, but it was also

---

[21] *See* Otis, *supra* note 19 (portraying the belief that despite the structure or type of a man's house, it remained his castle and thus free from government intrusion).
[22] *See* Otis, *supra* note 19 (illustrating that illegal searches took place prior to the writing of the Fourth Amendment because a man's house was less of a castle in America than in Great Britain).
[23] *See* Otis, *supra* note 19 (discussing the development of new laws and regulations in response to oppression by the British crown).
[24] *See Levy*, *supra* note 18, at 82 (noting that when presented with the ability to create law that mirrored that of the crown's rule, the colonists instead rejected precedent and employed different legislative principles).
[25] *See* Levy, *supra* note 18, at 83 (explaining the colonist's purpose for creating their own law in the New World).
[26] *See* Levy, *supra* note 18, at 82 (reiterating that colonists abolished general warrants and writs of assistance in favor of a more specific type of warrant).
[27] *See* Levy, *supra* note 18, at 93 (observing that other colonies such as Virginia and Pennsylvania followed Massachusetts' example and ended the use of general warrants and writs of assistance and implemented more specific warrants).
[28] *See* Friedman & Kerr, *supra* note 15 (noting that the Framers included the Fourth Amendment in the Bill of Rights after much deliberation over terminology).

true in decades ago as well, as proved by *Katz v. United States*.[29] This case reached the Supreme Court after government investigators bugged a public phone booth in order to intercept Katz's transmission of gambling information.[30] Katz argued that the government violated his Fourth Amendment rights through its intrusion into his private conversations.[31] This case remains relevant today over 50 years later because it established that the Fourth Amendment protects people, not specific places.[32] This case was also innovative because it established that physical intrusion was no longer necessary to constitute a search, and that searches could occur without physically entering into someone's home.[33] The Court wrote that "[w]hat a person knowingly exposes to the public, even in his own home or office, is subject to Fourth Amendment protection[,] [b]ut what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[34] Through this statement, the Court began to focus to what extent an individual perceives her privacy by narrowly defining the scope of the space she considers to be her home.[35]

The *Katz* case also remains relevant today because it established a new standard for the application of the Fourth Amendment.[36] The Court determined that the application of the Fourth Amendment depends on "whether the person invoking its protection can claim a 'justifiable,' a 'reasonable,' or a 'legitimate expectation of

[29] *See* Katz v. United States, 389 U.S. 347 (1967) (finding that what an individual seeks to preserve as private, even in an area accessible to the public such as a public telephone booth, may be constitutionally protected).
[30] *See id.* at 348 (describing how FBI investigators attached an electronic listening and recording device to the outside of a public phone booth in order to eavesdrop on the petitioner's conversations).
[31] *See id.* at 352 (reasoning that the petitioner's conversations were private even though they occurred in a public phone booth).
[32] *See id.* at 351 (stating one of the Supreme Court's major takeaways from the case).
[33] *See If These Walls Could Talk*, *supra* note 4, at 1927-28 (explaining how the case created the concept of the third-party doctrine which was innovative for the time period).
[34] *See* Katz, *supra* note 29, at 351 (dictating that the Fourth Amendment is not meant to protect a specific location, but instead exists in order to protect people from unreasonable search and seizure).
[35] *See If These Walls Could Talk*, *supra* note 4, at 1926-27 (explaining that *Katz* represented a shift in the Supreme Court's interpretation of the Fourth Amendment).
[36] *See If These Walls Could Talk*, *supra* note 4, at 1927 (repeating why *Katz* is still relevant in twenty-first century America).

privacy' that has been invaded by government action."[37] This standard is then broken down into a two-part inquiry.[38] The first question is "whether the individual, by his conduct, has 'exhibited an actual (subjective) expectation of privacy."[39] The majority paraphrased this question by asking whether the individual in question has shown that "he seeks to preserve [something] as private."[40] The second part of the inquiry is whether the "individual's subjective expectation of privacy is one that society is prepared to recognize as "reasonable." [41] The Court applied this new standard and ruled in favor of Katz because he "justifiably relied" on the expected privacy of the phone booth.[42]

B. The Fourth Amendment and Third Parties

It was not long after the Katz decision that the Court was forced to employ this standard in the case *Smith v. Maryland*.[43] This case arose after Baltimore police had the local telephone company install a pen register at its central office to record the phone numbers the suspect dialed, all without a warrant.[44] The petitioner moved to suppress all of the evidence collected by the pen register, but was denied and convicted.[45] The Court of Appeals affirmed the judgment,

---

[37] *See* Smith v. Maryland, 442 U.S. 735, 736 (1979) (listing the new standards for the interpretation of the Fourth Amendment after the *Katz* decision).
[38] *See id.* at 740 (providing further insight as to how the Court interprets and applies the Fourth Amendment to issues after the precedents established by the *Katz* decision).
[39] *See id.* at 740 (setting forth the first of the two-part inquiry utilized by the Court to address the Fourth Amendment).
[40] *See* Katz, *supra* note 29, at 351 (stating that what one "seeks to preserve as private . . . . may be constitutionally protected").
[41] *See* Katz, *supra* note 29, at 361 (Harlan, J., concurring) (describing that the second part of the two-part inquiry in that society recognizes one's expectation of privacy as reasonable).
[42] *See* Katz, *supra* note 29, at 353 (noting the Court's use of this two-party inquiry to rule that *Katz* "justifiably relied" on the privacy he expected to receive in the public phone booth).
[43] *See* Smith, *supra* note 37, at 745-46 (reasoning that an individual's expectation of privacy in an accessible place to the public must also be reasonable to be constitutionally protected).
[44] *See* Smith, *supra* note 37, at 736-37 (explaining the warrantless use and purpose of a pen register to record the phone numbers dialed by the petitioner).
[45] *See* Smith, *supra* note 37, at 737 (observing how the petitioner sought to suppress all the evidence and data collected by the pen register because the police instructed the phone company to install it without a warrant).

holding that "there is no constitutionally protected reasonable expectation of privacy in the numbers dialed into a telephone system and hence no search within."[46] Therefore, a warrant was not necessary because there was no search conducted in the first place.[47]

The Supreme Court applied the *Katz* standard and first questioned whether there was an invasion of the petitioner's property.[48] The Court ruled that because the installation of the pen register occurred at the central headquarters of the phone company, the government never intruded onto a constitutionally protected place, such as a residence.[49] Additionally, the Court determined that the petitioner had no "legitimate expectation of privacy" and thus failed the first part of the *Katz* inquiry.[50] The Court stated that people generally do not have an expectation that the phone numbers they dial will remain private, as placing a phone call requires the phone company's technology to connect lines.[51] The Court then ruled that the petitioner failed the second part of the *Katz* inquiry stating that "[e]ven if petitioner did harbor some subjective expectation that the phone numbers he dialed would remain private, the expectation is not one that society is prepared to recognize as reasonable."[52] The Court differentiated *Katz* from *Smith* by highlighting that in the former, where it ruled in favor of the petitioner, the government had the ability

---

[46] *See* Smith, *supra* note 37, at 738 (articulating that for a telephone call to be completed, the number dialed must be provided to the telephone company for the manual connection of the two lines).

[47] *See* Smith, *supra* note 37, at 738 (stating that police did not need a warrant in order to have the pen register installed because this action did not constitute a "search").

[48] *See* Smith, *supra* note 37, at 740 (providing that the Supreme Court used the two-part inquiry established in *Katz* for the *Smith* decision).

[49] *See* Smith, *supra* note 37, at 741 (contrasting the installation of the pen register at the phone company's physical location from an actual search of one's residence).

[50] *See* Smith, *supra* note 37, at 743 (offering that a caller cannot expect for the phone number to be kept private because of the nature of the completion of a telephone call).

[51] *See* Smith, *supra* note 37, at 743 (opining that the average person in the general population does not make a phone call while maintaining the belief that the phone number dialed will remain private information).

[52] *See* Smith, *supra* note 37, at 743 (elaborating that even if a caller expected the number that he dialed to remain private, the general population does not maintain this same view and thus would not accept such a belief as reasonable).

to intrude by listening to the content of the conversations in question.[53] This was not the case in *Smith* because the pen register merely recorded the phone numbers dialed, not the actual conversations of the phone calls.[54] The Court affirmed the ruling and stated that "[a] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[55]

C. The Fourth Amendment and Entry into the Private Home

The case *Kyllo v. United States*[56] demonstrates how the law developed further after *Smith*. This case concerned the suspected growing of marijuana inside a private home and the tactics that police officers utilized in their investigation.[57] Investigators knew that growing marijuana in a home required the use of heat lamps so they utilized a thermal imaging device to locate places of extreme heat within the suspect's house.[58] This methodology sparked the question as to whether the use of such a device constituted a traditional search within the meaning of the Fourth Amendment.[59] Complicating matters further was the fact that the police used the thermal imaging device from the public street to investigate the interior of a private home.[60] Police only sought a warrant to search the home *after* conducting their

---

[53] *See* Smith, *supra* note 37, at 741 (recognizing that there is a major difference between having the ability to listen to the actual content of the phone calls and only accessing the phone numbers dialed).

[54] *See* Smith, *supra* note 37, at 741 (contrasting the facts in *Katz* and *Smith* and discussing how they led to different rulings).

[55] *See* Smith, *supra* note 37, at 743-44 (upholding that the Supreme Court consistently follows this standard).

[56] *See* Kyllo v. U.S., 533 U.S. 27, 40 (2001) (investigating to what extent the use of technology invades personal privacy under the Fourth Amendment).

[57] *See id.* at 29 (referring specifically to the use of a thermal-imaging device aimed at a private home from a public street).

[58] *See id.* at 29 (explaining how investigators obtained evidence with neither a warrant nor a physical search of the petitioner's home).

[59] *See id.* at 34-35 (describing the issue of whether the use of a thermal imaging device constituted a search under the Fourth Amendment).

[60] *See id.* at 30 (discussing the scan only took a few minutes and revealed the roof over the garage and a side wall of the home were substantially warmer than the rest of the home).

investigation from outside the home.[61] They found over 100 marijuana plants inside the home and arrested Kyllo.[62] Kyllo then moved to have the thermal imaging evidence suppressed.[63] The Supreme Court ruled against Kyllo and stated that he had not demonstrated a subjective expectation of privacy.[64] He then appealed to the United States Court of Appeals for the Ninth Circuit, who upheld his conviction.[65] However, the Supreme Court granted certiorari and reversed the Court of Appeals' judgment.[66] In a 5-4 decision, the Court ruled that the use of the thermal imaging device constituted a search and that this particular search was unreasonable because the police did not have the necessary warrant when it was conducted.[67] The Court stated that "[a]t the very core of the Federal Constitution's Fourth Amendment stands one's right to retreat into one's own home and there be free from unreasonable government intrusion; with few exceptions, the question whether a warrantless search of a home is reasonable and hence constitutional must be answered 'no.'"[68]

Furthermore, the Court focused on the issue that police did not obtain a warrant until their goal was to step inside and physically search the house.[69] By the time a Federal Magistrate Judge issued a warrant, police already had evidence from informant tips, electricity

[61] *See* Kyllo, *supra* note 56, at 30 (providing that investigators only sought a warrant from a judge after completing the employment of the thermal imaging device from the exterior of petitioner's house).

[62] *See* Kyllo, *supra* note 56, at 30 (acknowledging that the petitioner was in the possession of over 100 illegal marijuana plants).

[63] *See* Kyllo, *supra* note 56, at 30 (stating the petitioner's attempt to have the thermal imagining evidence suppressed and his conditional guilty pleading).

[64] *See* Kyllo, *supra* note 56, at 30-31 (commenting that the district court originally ruled against the petitioner because it found that he did not successfully demonstrate a subjective expectation of privacy).

[65] *See* Kyllo, *supra* note 56, at 30-31 (recounting that upon appeal, the United States Court of Appeals for the Ninth Circuit vacated the petitioner's conviction).

[66] *See* Kyllo, *supra* note 56, at 31 (announcing that the Supreme Court granted certiorari and ruled on this case).

[67] *See* Kyllo, *supra* note 56 at 40-41 (summarizing that the Supreme Court ruled in favor of the petitioner and stated that the use of the thermal imaging device constituted a search and that subsequently a warrant was necessary).

[68] *See* Kyllo, *supra* note 56, at 31 (observing a long-held belief that an individual has the protected right to be private within his home as established in Silverman v. United States, 365 U.S. 505, 511 (1961)).

[69] *See* Kyllo, *supra* note 56, at 38-39 (emphasizing that the police officers would not have been able to know in advance of obtaining the warrant whether their search had been constitutional).

bills, and of course the images produced by the thermal imaging device.[70] The Court supported its reasoning by referring to a previous ruling where it stated:

> Any physical invasion of the structure of the home, 'by even a fraction of an inch,' [is] too much, and there is certainly no exception to the warrant requirement for the officer who barely cracks open the front door and sees nothing but the non-intimate rug on the vestibule floor. In the home, judicial precedent shows, all details are intimate details, because the entire area is held safe from prying government eyes.[71]

By this reasoning, the Court affirmed that despite the fact that the only details investigators obtained involved the temperature of locations in the house, such details remained "intimate" nonetheless because they were details of a private home.[72] Furthermore, the Court explained that it would have to develop a rule that determined what type of activities within the home were intimate and which were not.[73] The Court stated that it would not complete such a task, and even if they did, such jurisprudence would be ineffective because a police officer would have no method of knowing in advance if he was about to detect an intimate activity.[74] The officer would therefore be unable to know if he was conducting a constitutional search until after the completion of said search.[75]

---

[70] *See* Kyllo, *supra* note 56, at 30 (stressing that police investigators did not seek a warrant from a judge until after obtaining a substantial amount of evidence).

[71] *See* Kyllo, *supra* note 56, at 37 (setting forth that a police officer may not conduct a search in the slightest without a warrant).

[72] *See* Kyllo, *supra* note 56, at 38 (opining that although heat locations do not seem to be intimate details, they remain intimate because they exist as information gathered from inside the home).

[73] *See* Kyllo, *supra* note 56, at 38-39 (explaining that the Supreme Court would have to create a standard in order to determine what constitutes an intimate detail and what does not).

[74] *See* Kyllo, *supra* note 56, at 39 (elaborating on the previous sentence and stating the Supreme Court was not willing to create such a standard).

[75] *See* Kyllo, *supra* note 56, at 39 (developing further on the notion that the establishment of such a standard would be rendered pointless because an officer would not have the ability to know ahead of time if he was conducting a search of an intimate activity).

D. The Fourth Amendment and Smartphones

In *Riley v. California*,[76] a seemingly routine traffic stop sparked a Supreme Court case involving law enforcement's ability to search a smartphone under the Fourth Amendment.[77] Police officers pulled Riley over for having expired registration tags. [78] Soon after, the officer uncovered that Riley's license had been suspended, resulting in the officer impounding the vehicle.[79] Upon further examination of the vehicle, officers discovered two handguns hidden underneath the hood of the automobile.[80] This revelation resulted in Riley's arrest and the subsequent search of his smartphone.[81] While searching Riley's person for other weapons or contraband, officers happened upon his smartphone and began to examine its contents.[82] The officer found references to Riley's membership in the "Bloods" street gang in his text messages, prompting another officer specializing in gangs to further inspect the smartphone.[83] Authorities ultimately charged Riley with firing at an occupied vehicle, assault with a semiautomatic firearm, and attempted murder – all resulting from content obtained from his smartphone.[84] Prior to his trial, Riley's lawyers moved to suppress all of the evidence collected from his

[76] *See* Riley v. California, 134 S. Ct. at 2494-95 (2014) (emphasizing the reasonableness inquiry for expectation of privacy in Fourth Amendment claims).
[77] *See id.* at 2480 ("[W]hether the police may, without a warrant, search digital information on a cell phone?").
[78] *See id.* at 2480 (recalling the reason behind the police officer's decision to pull over Riley).
[79] *See id.* at 2480 (describing how the traffic stop developed from a routine stop to one featuring the arrest of the driver).
[80] *See id*. at 2494-95 (discussing further conditions that led to Riley's arrest and the subsequent charges he faced).
[81] *See* Riley, *supra* note 76, at 2480-81 (making the connection between the expired registration tags and the gang ties discovered through the examination of Riley's smartphone).
[82] *See* Riley, *supra* note 76, at 2480-81 (establishing the pattern of events that occurred after police officers decided to arrest Riley because of his suspended driver's license).
[83] *See* Riley, *supra* note 76, at 2480-81 (summarizing the officer's discoveries and how they obtained evidence tying Riley to the "Bloods" gang; these discoveries would eventually lead to authorities pressing several charges against him).
[84] *See* Riley, *supra* note 76, at 2481 (introducing the felonies charged against Riley, including firing at an occupied vehicle, assault with a semiautomatic firearm, and attempted murder).

smartphone, contending that such a search violated his Fourth Amendment rights.[85]

The Supreme Court ruled in favor of Riley, affirming the judgment to suppress the evidence, thus reversing the guilty conviction.[86] The Court based its decision on reasonableness, stating that "[t]he ultimate touchstone of the Fourth Amendment is reasonableness[,] [and] [w]here a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing, reasonableness generally requires the obtaining of a judicial warrant."[87] The Court held that while Riley's arrest was lawful, the subsequent search of his smartphone was not.[88] The Court made this decision based on the fact that unlike a knife or firearm, a smartphone alone is not a weapon with which an arrestee can injure a police officer.[89] It reasoned that an immediate search of the smartphone was unnecessary and therefore unreasonable.[90] Furthermore, the Court's holding was not that information and data found on a smartphone is immune to police searches, instead, it held that a warrant is generally necessary before such investigation can begin.[91]

On November 22, 2015, first responders answered a call at the residence of James Andrew Bates of Bentonville, Arkansas.[92] There,

---

[85] *See* Riley, *supra* note 76, at 2481 (addressing the defensive strategies employed by Riley's counsel, including a motion to suppress all of the evidence officers obtained from his smartphone).

[86] *See* Riley, *supra* note 76, at 2495 (announcing the Supreme Court's holding, which ruled in favor of Riley and reversed his guilty conviction after affirming the lower court's judgment to suppress the smartphone evidence).

[87] *See* Riley, *supra* note 76, at 2482 (explaining that the Supreme Court focused much of its decision on the concept of reasonableness, and describing what comprises reasonableness in the realm of police searches).

[88] *See* Riley, *supra* note 76, at 2495 (providing the Supreme Court's holding that reversed and remanded the appellate court decision).

[89] *See* Riley, *supra* note 76, at 2485 (reasoning that once a police officer physically secures a smartphone, it ceases to be a threat to his personal safety and security).

[90] *See* Riley, *supra* note 76, at 2485 (echoing that a smartphone alone is not a hazard to a police officer's safety).

[91] See Riley, *supra* note 76, at 2479 (emphasizing that although the Court ruled to suppress Riley's smartphone evidence, it did not rule that data collected from such a device is immune from all police searches).

[92] *See* Zuzanna Sitek & Dillon Thomas, *Bentonvillle PD Says Man Strangled, Drowned Former Georgia Officer*, 5 NEWS ONLINE (Feb. 23, 2016), *archived at* https://perma.cc/GQ5N-8ZNB (providing the time and location of the police investigation in response to the 911 call); *see also* Amy B. Wang, *Can Alexa Help Solve a Murder? Police Think So – But Amazon Won't Give Up Her Data*, L.A.

they found the dead body of Victor Collins, 47, of Centerton, Arkansas submerged in the residence's hot tub.[93] Police soon became suspicious of Bates and began their official investigation with the search of his residence.[94] They stumbled upon Bates' Amazon Echo and then commenced a legal battle with the online superstore to obtain the device's records.[95] This sparked an entirely new legal conundrum involving one's privacy within her smart home device.[96] Among the new issues arising out of this legal battle is the question of why Amazon collects and stores Echo owner's data in the first place.[97] Furthermore, an entirely new realm of privacy issues may now exist because of the collection and storage of this information from within the home.[98] David C. Vladek perhaps said it best when he opined, "historical boundaries for information-collection are under siege by evolving technology."[99] The precedent established in the nations past

---

TIMES (Dec. 28, 2016), *archived at* https://perma.cc/ZZG8-AUZZ (commenting on the novelty of this murder investigation in its quest to obtain data from an Amazon Echo device).

[93] *See* Sitek & Thomas, *supra* note 92 (describing what police officers encountered when they arrived at the suspect's home).

[94] *See* Sitek & Thomas, *supra* note 92 (detailing early suspicions of foul play which led to a search of Bates' home).

[95] *See* Amy B. Wang, *Police Land Amazon Echo Data in Quest to Solve Murder*, CHICAGO TRIBUNE (Mar. 9, 2017), *archived at* https://perma.cc/K8E4-5EG7 (considering the legal debate regarding privacy that has arisen in consequence of the Collins murder); *see also* Eliott C. McLaughlin, *Suspect OKs Amazon to Hand Over Echo Recordings in Murder Case*, CNN, (Apr. 26, 2017), *archived at* https://perma.cc/S5W8-PKTT (reporting that Bates consented to Amazon turning over data from his Echo device to authorities).

[96] See McLaughlin, *supra* note 95 (questioning the extent of one's privacy in her home); *see also* Margot E. Kaminski et al., *Symposium Essays from The State of Cyberlaw: Security and Privacy in the Digital Age: AVERTING ROBOT EYES*, 76 MD. L. REV. 983, 993 (2017) (providing information about Amazon's motion to quash the search warrant and its argument that "rumors of an Orwellian federal criminal investigation into the reading habits of Amazon's costumers could frighten countless potential customers").

[97] *See* Brian Heater, *Can Your Smart Home be Used Against You in Court?*, TECH CRUNCH (Mar. 12, 2017), *archived at* https://perma.cc/WJ3N-SEZ3 (stating that Amazon collects and stores what is presumed to be private information from its Echo users).

[98] *See* Gerald Sauer, *A Murder Case Tests Alexa's Devotion to Your Privacy*, WIRED (Feb. 28, 2017), *archived at* https://perma.cc/9CBW-28SF (developing on the potential mishaps of the collection and storage of Echo data).

[99] *See* David C. Vladeck, *Consumer Protection in an Era of Big Data Analytics*, 42 OHIO N.U. L. REV. 493, 500 (2016) (suggesting that despite their claims otherwise,

may no longer be relevant thanks to the advanced technology in today's smart home because the current law does not address the rapidly paced technological developments of the twenty-first century.

III. Facts

It may be difficult for some readers to connect the dangers of Echo home use with the privacy precedent that cases such as *Katz*, *Smith*, *Kyllo*, and *Riley* establish. However, one must only examine the extent of the Echo's abilities to understand the threat to one's privacy that its use entails. The existence and purpose of the Echo may seem innocuous enough as it serves as a personal in-home assistant meant to increase its user's convenience, yet it is vital to recall that unlike a human assistant that goes home at the end of every shift, the Echo is always listening.[100] Because the device is in a constant state of vigilance to begin its services at the mention of the wake word, it also has the capability to "overhear" much more than what its owner intends.[101] This becomes problematic because users do not enjoy the privacy rights that they presume protect them when they make carefree remarks around their Echo.[102] In a situation where authorities may attempt to seize data recorded by the Echo, users will face difficulty because in order to challenge a search under the Fourth Amendment, "one must have an expectation of privacy that society recognizes as reasonable."[103]

---

companies such as Apple and Amazon use personal information for marketing purposes).

[100] *See* Eric Boughman et al., *"Alexa, Do You Have Rights?": Legal Issues Posed by Voice-Controlled Devices and the Data They Create*, A.B.A. (Nov. 19, 2017), *archived at* https://perma.cc/P42X-Q4VS (highlighting that the device is always listening for its wake word to be said).

[101] *See id.* (noting even though the device begins recording once its wake word is said, users may accidently trigger the feature by saying the wake word in passing or unintentionally).

[102] *See id.* (opining that Echo users may mistakenly say the wake word and thus begin recording conversations that are meant to remain private).

[103] *See id.* (detailing that as laid out in the *Katz* decision, one must have a socially-recognized reasonable expectation of privacy in order to be able to successfully challenge a search under the Fourth Amendment).

It is unlikely for such expectation of privacy to be deemed reasonable once one considers the Echo's user agreement.[104] Commentator Eric Boughman explained that "[t]ypical privacy policies provide that the user's personal information may be disclosed to third parties who assist the service provider in providing services requested by the user, and to third parties."[105] Thus, this disclosure to third parties is critical as it effectively eliminates an Echo user's reasonable expectation of privacy because "with few exceptions, one has an expectation of privacy in one's own home, but broadly, there is no reasonable expectation of privacy in information disclosed to a third party."[106] With this understanding, it is unlikely that society would recognize such an expectation of privacy to be reasonable.[107]

Nevertheless, the question behind why the Echo's programming includes this 'always-listening' feature remains.[108] Amazon and other companies that produce voice-recognition devices such as the Echo include this capability in their products as a method to improve the products' ability to comprehend voices and, therefore, fulfill requests as well.[109] This means that whenever a user speaks the "wake word," the Echo wakes up, records the statement, and then transmits the recording file to its home base or cloud.[110] This may not

---

[104] *See id.* (claiming that one could not possibly consider such privacy to be reasonable after reading and understanding the terms of service agreements proscribed with devices such as the Echo).

[105] *See* Boughman, *supra* note 100 (describing how privacy policies enable voice data to be shared with third parties).

[106] *See* Boughman, *supra* note 100 (explaining that Fourth Amendment rights do not apply to information or data that is shared with third parties of any sort).

[107] *See* Boughman, *supra* note 100 (concluding that with this understanding, society will not find it reasonable).

[108] *See* Arielle M. Rediger, *Always-Listening Technology: Who is Listening and What Can Be Done About It?*, 29 LOY. CONSUMER L. REV. 229, 230 (2017) (discussing the potential legal issues involved with new technology that has the capability to always be listening to its user).

[109] *See If These Walls Could Talk*, *supra* note 4, at 1940 (examining why Amazon records and saves all user inquires). "Recorded utterances and requests are stored on that respective company's servers and associated with the user's account, so as to enable the device to better recognize a user's voice or speech patterns and respond to commands more seamlessly." *Id.*

[110] *See If These Walls Could Talk*, *supra* note 4, at 1940 (elaborating on how spoken words are turned into voice data that is transmitted to an online storage system known as the cloud); *see also Not in Front of the Telly: Warning Over "Listening" TV*, BBC NEWS (Feb. 9, 2015) *archived at* https://perma.cc/5MUN-Q27H (explaining how the

appear to be problematic until one considers that Amazon stores the data unless the user manually deletes it.[111] The ability to delete this data does not come without its hindrances, as Amazon utilizes this "history" to make the Echo "smarter" by learning what the user asks for and how often the user asks for it.[112] This connection may spark some users to wonder what is the major concern if all Amazon uses one's personal data for is the improvement of the Echo, for the purpose of user convenience.[113] However, some Echo owners remain disturbed by the product's ability to make connections between inquiries and personal information.[114] For example, Echo usage allows Amazon to create comprehensive profiles of the user and the user's activities.[115] This means that the Echo can create profiles based on personal health, location, activities, and even political leanings through the use of health monitoring applications, calendars, to-do lists, and even including which news websites are frequented.[116] The ability to construct such a detailed personal profile disturbs some consumers; what Amazon and other smart home device producers can do with such data only frightens users further.[117]

Samsung Smart TV listens to owners' statements at all times, resulting in unintended commands and queries).

[111] *See If These Walls Could Talk*, *supra* note 4 (noting that similarly to one's online search history, voice data can only be removed from the cloud if a user manually deletes it herself).

[112] *See* Sharon D. Nelson & John W. Simek, *Are Alexa and Her Friends Safe for Office Use?*, LAW PRACTICE, 1, 26-29 (Sept./Oct. 2017) (demonstrating what devices such as the Echo do with the stored voice data).

[113] *See id.* at 29 (questioning whether it is truly problematic that the Echo and similar devices store and keep all voice data within their cloud systems).

[114] *See If These Walls Could Talk*, *supra* note 4, at 1940-41 (demonstrating one Echo user who had a conversation with his wife about babies, to then have an advertisement for diapers appear on his Kindle reading device days later).

[115] *See If These Walls Could Talk*, *supra* note 4, at 1940 (expanding upon how the Echo's storing of data based on interactions with users allows it to construct a personal profile); *but see* Anita L. Allen, *Protecting One's Own Privacy in a Big Data Economy*, 130 HARV. L. REV. FORUM 71, 74 (2016) (suggesting that the collection of personal data may have positive effects in the healthcare world, as such data would provide doctors with a clearer picture as to how to treat patients).

[116] *See If These Walls Could Talk*, *supra* note 4 (providing examples of how the Echo can create a personal profile for its user just from the questions and inquiries asked of it).

[117] *See If These Walls Could Talk*, *supra* note 4 (understanding that users may worry about the use of their data).

Aside from the ability to produce personal profiles based on user's requests and inquiries, the Echo and similar devices may also be able to "provide companies with leading indicators, such as information about the user's state of mind and triggering events that may result in the desired interactions with a company."[118] This means that the Echo may be able to record and then analyze the user's voice's pitch, amplitude, and tone and, therefore, deduce the user's emotional status.[119] Such data can become a privacy issue when companies then use it in algorithms to suggest certain products or services to the user.[120] Commentator Margot Kamiski explains that "[r]obots may, like other information technology, enable individuals or companies to take information that has been shared in one context and share or use it in another."[121] Users often do not realize that the terms of service for some digital assistants specifically state that their voice recordings may be used to not only improve the digital assistant itself, but also to be shared with third parties.[122] This data is then shared with or sold to third party companies who use it to create predictive models.[123] Commentator Laura K. Donohue explains that "our reliance on industry and third-party providers to service the needs of daily life has made much more of our personal information, as well as new kinds of personal data, vulnerable to government collection."[124] This means that while consumers may view the government's newfound ability to

[118] *See* Boughman, *supra* note 100 (introducing other capabilities of the Echo beyond the creation of personal profiles).
[119] *See* Boughman, *supra* note 100 (describing how the Echo can take voice data and turn it into information regarding emotion).
[120] *See If These Walls Could Talk*, *supra* note 4, at 1940-41 (providing an example for how devices such as the Echo take input data and then determine what types of products might interest users).
[121] *See* Kaminski, *supra* note 96, at 994 (elaborating on the ability of countless smart devices to come to conclusions regarding personal information based on searches and inquiries).
[122] *See* Boughman, *supra* note 100 (establishing that there are terms of service when using voice recording technology).
[123] *See* Boughman, *supra* note 100 (examining what companies such as Amazon do with user data once they collect it from smart devices such as the Echo). "The influx of this data can fundamentally change both the strength and the nature of the predictive models that companies use to inform their interactions with consumers." *Id.*
[124] Laura K. Donohue, *The Fourth Amendment in a Digital World*, 71 N.Y.U. ANN. SURV. AM. L. 553, 555 (2017) (discussing the effects of technology on our daily lives including the implications of digital dependence).

collect data as a risk to personal privacy, there is probably little choice otherwise because of modern civilization's dependence on smart devices and their accompanying applications and abilities.[125] These predictive models use statistics to forecast which types of products or services a user may be interested in purchasing.[126] Boughman further explains that "[e]ven if digital assistants only record interactions between the user and the device, the richness of voice data means that predictive models become finely-tuned to each individual user."[127] This means that every interaction with a digital assistant, such as an Amazon Echo, may help build a unique user profile based on the use of predictive modeling.[128] Through such predictive modeling, data is exposed to third parties, thus effectively eliminating any right to privacy.[129]

IV. Analysis

To best predict how courts in the future will treat the Amazon Echo, we must examine the phenomenon in light of past Fourth Amendment cases.[130] How the Amazon Echo and its accompanying data is treated will depend on how courts interpret precedent

---

[125] *See id.* at 555 (expanding on the notion that society depends on the online world for school, work, social interactions, hobbies, and other pursuits).

[126] *See* Boughman, *supra* note 100 (providing further explanation regarding the use of predictive models and how they are formed); *see also* Ann T. McKenna, *Where There is No Darkness: Technology and the Future of Privacy*, 65 RUTGERS L. REV. 1041, 1088 (2013) (providing Amazon as a an example of a company that utilizes consumer contact and credit card information to recommend future items).

[127] Boughman, *supra* note 100 (explaining how the properties and qualities of voice data enable devices such as the Echo to develop further personal profiles with their users).

[128] *See* Boughman, *supra* note 100 (discussing the concept and purpose ofpredictive modeling).

[129] *See* Boughman, *supra* note 100 (noting that digital assistants may use technologies to "avoid becoming subject to privacy regulations"); *see also* Kristen M. Beasley, *Up-Skirt and Other Dirt: Why Cell Phone Cameras and Other Technologies Require a New Approach to Protecting Personal Privacy in Public Places*, 31 S. ILL. U. L. J. 69, 70 (2006) (relaying to readers that while Americans have a reasonable expectation of privacy in their homes, they waive this expectation in the public sphere).

[130] *See* Michael Harrigan, *Privacy Versus Justice: Amazon's First Amendment Battle in the Cloud*, 45 W. ST. L. REV. 91, 92 (2017) (hypothesizing that more domestic violence cases will result in a higher percentage of guilty verdicts if courts allow the government to gain access to Echo data).

established by Supreme Court decisions on the issue of privacy.[131] For example, *Katz v. United States* established that the Fourth Amendment protects people, not specific places, such as the interior of one's home.[132] This precedent is meaningful in relation to the Amazon Echo because it essentially determines that one's home and what occurs within it is not automatically protected by the Fourth Amendment.[133] Instead, it focuses on the protection of an individual's personal liberty and not the guaranteed protection in a certain location, such as a private home.[134] Thus, since one's home is not automatically protected by the Fourth Amendment, it is unlikely that the data collected by a smart home device would enjoy any protection whatsoever.[135] The Court also determined that physical intrusion was no longer necessary to constitute a search.[136] This is significant to the existence of the Amazon Echo because it means that searches can occur without physically going into a private home.[137] Thus, the physical location of the device cannot protect it from government intrusion.[138] The fact

[131] *See* Katherine E. Tapp, *Smart Devices Won't Be "Smart" Until Society Demands an Expectation of Privacy*, 56 U. Louisville L. Rev. 83, 107 (2017) (contrasting the limits of traditional search and those that may arise out of smart home or device technologies).

[132] *See* Katz, *supra* note 29, at 351 (reiterating that the Fourth Amendment serves to protect people from unreasonable searches, not specific places or locations).

[133] *See* Katz, *supra* note 29, at 351 (establishing that activities within a private home are not necessarily protected by the Fourth Amendment).

[134] *See* Katz, *supra* note 29, at 351 (distinguishing between how the *Katz* Court interpreted the implementation of the Fourth Amendment versus how the public interprets the Fourth Amendment).

[135] *See* Katz, *supra* note 29, at 351 (claiming that since the Fourth Amendment does not necessarily protect a location, it is unlikely that activity that occurs in said location is protected).

[136] *See* Katz, *supra* note 29, at 353 (explaining that the reach of the Fourth Amendment cannot turn upon the presence or absence of a physical intrusion into a location).

[137] *See* Kyllo, *supra* note 56, at 40 (concluding that government authorities may conduct a warrantless search without entering a private residence using technology readily available to the public, but noting that such searches are impermissible when said technology is not "in general public use"); *see also* Steven L. Friedland, *Drinking from the Firehouse: How Massive Self-Surveillance from the Internet of Things is Changing the Face of Privacy*, 119 W. VA. L. REV. 891, 892 (2017) (describing how the Internet of Things, an aggregation of networks connected by the internet, "creates consensual mass self-surveillance" in domains including smart homes).

[138] *See* Katz, *supra* note 29, at 351 (repeating that the Fourth Amendment protects people, not places).

that it exists within an individual's private home alone is not enough to prevent the government from gaining access to it and its accompanying data.[139]

The *Katz* Court also stated that "[w]hat a person knowingly exposes to the public even in his own home or office, is not a subject of Fourth Amendment protection."[140] If courts interpret and implement this statement, then anything that Alexa records or picks up on will subsequently be considered in the category of "expos[ed] to the public."[141] The terms of use ensure that Echo owners are legally on notice that anything their device records is transmitted back to Amazon.[142] Whether an Echo owner actually reads the user agreement and thus has actual knowledge of this practice is irrelevant.[143] Since Amazon includes such a provision in its Terms of Use, it is subsequently permitted to receive and store personal information from its users.[144] If future courts decide to implement this ruling, then it is unlikely that Echo data will receive the Fourth Amendment protection that it covets.[145] The Court specifically stated that the Fourth Amendment does not protect any type of knowingly-exposed information, even if it comes from within a private home or office.[146] Although the Court was unaware of its future accuracy, it explicitly addresses the Echo with this statement because a person knowingly

---

[139] *See* Katz, *supra* note 29, at 351 (noting that physical location alone cannot protect an item or area from being searched by government authorities).

[140] *See* Katz, *supra* note 29, at 351 (detailing that an individual cannot expect to receive Fourth Amendment protection for anything that he knowingly exposes to the public).

[141] *See* Sauer, *supra* note 98 (developing further on why Amazon and other smart home product companies retain records of all inquiries, suggesting that if Google has good-faith reasons for disclosing their data reasonably necessary to meet certain laws or regulations, they will retain the records).

[142] *See* Bradley, *supra* note 13 ("Amazon will not release customer information without a valid and binding legal demand properly served on [them].").

[143] *See* Rediger, *supra* note 108, at 250 ("[T] likelihood that the consumers will read through all of the disclaimers, privacy agreements, and litany of other warnings provided to them is slim to none.").

[144] *See* Rediger, *supra* note 108, at 250 (listing the provisions to Amazon's terms of use for Alexa).

[145] *See* Rediger, *supra* note 108, at 251 (stating that "always-listening technologies" are likely to earn Fourth Amendment protections in a future Supreme Court case).

[146] *See* Katz, *supra* note 29, at 351 (elucidating that the Fourth Amendment will not protect knowingly-exposed material regardless of the location of its source).

transmits information to the public whenever he or she utilizes the Echo at home.[147]

Conversely, courts may also emphasize the second part of the previous statement, which declares, "but what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[148] If a court were to implement this approach, then it is much more likely that data collected from an Amazon Echo would receive protection from government intrusion.[149] Although users should be aware that Amazon receives and stores all of their Echo inquiries and requests, it is nearly certain that widespread ignorance of this fact exists among the user population.[150] Such a bold statement can only be made when one considers how often he or she actually reads any type of user agreement before clicking the proverbial "I agree to the terms and conditions" box.[151] Thus, users could argue that even though they should have been aware of the fact that Amazon received all their seemingly private information, they were not and, therefore, sought to preserve such information as private.[152] Furthermore, those making such an argument will likely attack the part of the sentence that says, "even in an area accessible to the public."[153] They may point out that the statement provides

[147] *See* Sauer, *supra* note 98 (recounting that every inquiry made by a user is received and stored by Amazon).

[148] *See* Katz, *supra* note 29, at 351-52 (suggesting that future courts should interpret the Fourth Amendment in such a way that closely scrutinizes why the person is seeking Fourth Amendment protection, like when they would reasonably expect privacy in a public telephone booth).

[149] *See* Katz, *supra* note 29, at 351-52 (inferring that consumers would expect protection from government intrusion from their Amazon Echo, because it is seen as a private device)*; see also* Rediger, *supra* note 108, at 251 (arguing that courts may grant the Echo further protection if they determine that its user sought to keep his inquiries and requests as private); *but see* Lipton, *supra* note 10, at 413-14 (suggesting that users of items such as the Samsung SmartTV or Hello Barbie consent to the interception of their data regardless of whether they read the terms of use agreements).

[150] *See* Rediger, *supra* note 108, at 250 (declaring that the percentage of Echo users who read the terms of use before utilizing the product remain extremely low).

[151] *See* Rediger, *supra* note 108, at 250 (claiming that most consumers rarely read terms of use statements or user agreements before using a product or service).

[152] *See* Rediger, *supra* note 108, at 251 ("Users have both a subjective and objectively reasonable expectation of privacy in using [Amazon Echo].").

[153] *See* Katz, *supra* note 29, at 351 (expressing that what an individual seeks to preserve as private may still receive Fourth Amendment protection despite it being publicly accessible).

protection to their information because, although they have made it accessible to a third party, they have not necessarily made it accessible to the public.[154] That is to say that users have inadvertently provided their personal data to Amazon only, and their information is not made known to the general public. [155] Proponents of this approach will bolster their argument by suggesting that the Court's statement did, indeed, protect their personal information by including this specific detail.

The Supreme Court implemented a two-part inquiry in *Katz*.[156] The first part questioned "whether the individual, by his conduct, has 'exhibited an actual expectation of privacy.'"[157] The Court broke this part down further and asked whether the individual sought to preserve something as private.[158] Such a question requires further investigation into the expectations possessed by Echo owners.[159] Boughman comments that "[y]ou have an expectation of privacy in your home, and I have a big problem that law enforcement can use the technology that advances our quality of life against us."[160] This suggests that since people have an expectation of privacy in their homes, then this expectation of privacy also extends to their personal devices such as the Echo.[161] Thus, users may argue that they do, indeed, seek to preserve something as private: the sanctity of unobstructed home

---

[154] *See If These Walls Could Talk*, *supra* note 4, at 1925 (testifying that information relinquished to third party is no longer considered private).

[155] *See If These Walls Could Talk*, *supra* note 4, at 1924-25 (differentiating between private information and information released to a third party).

[156] *See* Katz, *supra* note 29, at 361 (giving an overview that the two-part test that has a subjective and objective component).

[157] *See* Katz, *supra* note 29, at 361 (applying the first part of a "twofold requirement" used when answering questions about the Fourth Amendment's protection of people instead of places).

[158] *See* Katz, *supra* note 29, at 351 (finding that based on precedent established by past Supreme Court cases, what an individual seeks to preserve as private, even in areas accessible to the public, may be constitutionally protected).

[159] *See* Boughman, *supra* note 100 (clarifying that with few exceptions, one has an expectation of privacy in one's home).

[160] *See* Boughman, *supra* note 100 (commenting that technology now raises a question whether individuals should expect privacy in their communications with voice-activated assistants).

[161] *See* Boughman, *supra* note 100 (contending that the general expectation of privacy within the home extends to an expectation of privacy for Echo inquiries among users).

life.[162] Whether a court would agree with such a claim remains a separate issue.[163] However, if a court were to implement the approach used in *Katz*, then it is likely that this argument would be successful in preserving this privacy expectation.[164] The Supreme Court stated that "[n]o 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 protections of the Fourth Amendment, since one who occupies it is entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world."[165] A court could translate this statement into one concerning the words uttered to an Echo device, and then conclude that the Fourth Amendment protects such communication.[166] The second part of the inquiry asks whether an individual's subjective expectation of privacy is one that society is prepared to recognize as reasonable.[167] The case of Alexa raises the question of whether society truly is knowledgeable enough about this technology to be able to make such a determination.[168] Perhaps the best method to gauge whether society is knowledgeable is to examine what its opinion regarding devices such as the Echo is in the first place.[169] Amazon has sold over ten million devices to date, which, while

---

[162] *See If These Walls Could Talk*, *supra* note 4, at 1940-41 (arguing that the use of smart home devices might entail the voluntary conveyance of the sanctity of home life to third parties).

[163] *See If These Walls Could Talk*, *supra* note 4, at 1942 (posing the "natural question" of "[W]hat is the Court to make of the smart home?").

[164] *See* Katz, *supra* note 29, at 352 (contending that when a person enters into a phone booth, he seeks to preserve his privacy and expects that his conversation will not be heard, despite the possibility that he may be visible within the booth).

[165] *See* Katz, *supra* note 29, at 352 (claiming that reading the Constitution more narrowly would be "to ignore the vital role that the public telephone ha[d] come to play in private communication").

[166] *See* Katz, *supra* note 29, at 358 (demonstrating a court's finding that one has a constitutionally protected expectation of privacy regarding words spoken to an Echo device).

[167] *See* Katz, *supra* note 29, at 361 (Harlan, J., concurring) (contending that society recognizes that a man has the subjective expectation of privacy within his own home).

[168] *See* Boughman, *supra* note 100 (proffering that because society has experience with other smart devices, it may be able to make some determination about the degree of privacy the Echo deserves).

[169] *See* Bradley, *supra* note 13 (pointing to Amazon Echo's FAQ section, which suggests that there is a high degree of unknown about the device); *see also Alexa FAQs*, AMAZON (2018), *archived at* https://perma.cc/99AW-XFGS (providing more detail on how the Echo devices work).

impressive, represents only a minor fraction of the population.[170] With such a small percentage of the population owning the device, it is unlikely that the population as a whole would be prepared to recognize this expectation of privacy as reasonable.[171] Developments such as the Echo are examples of "dramatic technological change" that will likely lead to "periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes."[172]

In *Smith v. Maryland*, the Supreme Court held that the police's use of a pen register did not violate the petitioner's constitutional rights because it was not an intrusion into a constitutionally protected place, such as a private home.[173] This ruling determined that the dialing of a phone number was not a protected private act, and that instead it was akin to releasing information to a third party.[174] The Court stated, "A person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[175] Unfortunately for Smith, the Court found that the physical act of dialing a phone number translated to voluntarily handing information to a third party.[176] In the case of the Echo, a similar question exists, that being whether releasing information into the cloud is the equivalent of dialing a phone number.[177] If courts find that it is, then it is possible that they will rule

[170] *See* Weinberger, *supra* note 5 (observing the number of Echo devices sold as of May 2017).
[171] *See* Bradley, *supra* note 13 (inferring that the echo remains a mystery to a vast majority of the population).
[172] *See* McKenna, *supra* note 125 (expanding upon the fact that developing technology may alter the assumption made in *Katz* that states a hypothetical reasonable person exists).
[173] *See* Smith, *supra* note 37, at 738 ("[T]here is no constitutionally protected reasonable expectation of privacy in the numbers dialed into a telephone system and hence no search within the Fourth Amendment is implicated by the use of a pen register ").
[174] *See* Smith, *supra* note 37, at 743 (explaining that the expectation of privacy while dialing a phone number differs from the expectation of privacy in the contents of a phone conversation).
[175] *See* Smith, *supra* note 37, at 743-44 (stressing that the court has consistently held that there is no longer an expectation of privacy once information is voluntarily exposed to third parties).
[176] *See* Smith, *supra* note 37, at 742 (observing that all telephone users "convey" phone numbers and thus personal information to the phone company whenever they dial a phone number).
[177] *See* Sauer, *supra* note 98 (outlining Amazon's practice of retaining Echo inquiries in the cloud).

in similar fashion to that of the *Smith* ruling.[178] This would likely mean that any inquiry made to Alexa would be interpreted as the same as dialing a telephone number.[179] Thus, if courts were to interpret this action as so, then any inquiry and subsequent information given to Alexa would also be voluntarily released to third parties as well.[180] Devices such as the Echo will require that courts "overhaul or discard" the third party doctrine first established by *Smith*.[181] In conclusion, it can be inferred that courts would again determine that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[182]

The case *Kyllo v. United States* determined that "any physical invasion of the structure of the home by even a fraction of an inch is too much [that] [i]n the home, judicial precedent shows all details are intimate details, because the entire area is held safe from prying government eyes."[183] If a court were to implement this finding in future cases concerning the Amazon Echo, then it appears that all inquiries would be protected from outside intrusion.[184] The *Kyllo* Court based its decision on the notion that all details are intimate because they occur within the privacy of one's home.[185] If a court were to conclude in the same manner, it can be assumed that it would rule that any Echo data would also fall into the category of said intimate

---

[178] *See* Smith, *supra* note 37, at 743-44 (reasoning that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties).

[179] *See* Sauer, *supra* note 98 (explaining Amazon's practice of logging and retaining all Alexa inquiries).

[180] *See* Sauer, *supra* note 98 (discussing that typical privacy policies provide that the user's personal information may be disclosed to third parties who assist the service provider in providing services requested by the user).

[181] *See* McKenna, *supra* note 125, at 1070 (expressing that modernity's communication and digital devices now require courts to interpret the third party doctrine in a revised manner that differs from that of the 1970s); *but see* Smith, *supra* note 37, at 744-45 (describing how the phone company's decision to change technologies does not require the Court to change third party doctrine expectations).

[182] *See* Smith, *supra* note 37, at 743-44 (maintaining that a person does not have a legitimate expectation of privacy for any information that he or she turns over to a third party).

[183] *See* Kyllo, *supra* note 56, at 37 (citing Silverman v. United States, 365 U.S. 505, 512 (1961) and discussing the importance of privacy in own's home).

[184] *See* Kyllo, *supra* note 56, at 38 (arguing that any detail was intimate because it was a detail of the private home).

[185] *See* Kyllo, *supra* note 56, at 38 (reiterating that any detail from within the home is intimate based solely on its origin).

details and thus receive the same protection granted to *Kyllo*.[186] Additionally, the *Kyllo* Court stated that it would not determine what types of activities are intimate and what types are not.[187] This decision would likely further protect inquiries made to Alexa, as courts would not examine each inquiry, but instead provide a blanket of protection. The facts of *Riley v. California* present perhaps the best indication on how courts may rule when first presented cases concerning Amazon Echo data.[188] There, the Supreme Court determined that "police generally may not, without a warrant, search digital information on a cell phone seized from an individual who has been arrested." [189] Because the *Riley* facts involving the search of a smart device relate so closely to issues relating to privacy and the Amazon Echo, it is likely not far-fetched to predict that courts will rule in a similar manner in the future.[190] Thus, *Riley* proved that while digital data presents new challenges to law enforcement and to the law in general, it deserves the same protection that tangible items receive.[191] The Court stated that "[t]he fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought."[192] Therefore, it is very well possible that courts will require warrants before enabling authorities to access data stored in smart devices such as the Amazon Echo.

In respect to James Bates's case, it is difficult to say how a court might have ruled because he agreed to have Amazon release his

---

[186] *See* Kyllo, *supra* note 56, at 38 (stating that such an approach would be wrong in principle because, in the sanctity of the home, all details are intimate details).

[187] *See* Kyllo, *supra* note 56, at 38-39 (proscribing that the Supreme Court was not willing to differentiate between intimate and non-intimate details).

[188] *See* Riley, *supra* note 76, at 2477 (understanding the need for additional warrant when it comes to technology).

[189] *See* Riley, *supra* note 76, at 2477 (dictating the general conclusion of the case, being that police officers must obtain a warrant before searching an arrested individual's cell phone).

[190] *See* Riley, *supra* note 76, at 2491 (discussing the emergence of smartphones and other technologically advanced devices that make use of the digital cloud).

[191] *See* Riley, *supra* note 76, at 2485 (comparing the associated risks with different pieces of evidence such as a knife or razor and the data found on a smartphone).

[192] *See* Riley, *supra* note 76, at 2495 (asserting that twenty-first century items deserve the same protections as those proscribed by the Founding Fathers despite the fact that they would have never been able to conceptualize them).

Alexa inquiries to authorities.[193] However, had he refused to do so, it is possible that Arkansas courts would have utilized the cases discussed above to evaluate Bates' privacy in this murder investigation.[194] In the future when similar situations arise, it is likely that a long court battle will ensue before either prosecutor or defendant wins its argument.[195] Nevertheless, the next time a smart home device offers authorities potentially incriminating evidence, they will go to court and battle against the defendant, establishing a precedent that allows government agencies access to information and data connected to devices like the Amazon Echo.[196] Future courts will rule in favor of investigating authorities because developing technology has forced the law to appropriately adapt in countless instances in the past, and there is nothing to suggest that such a trend would not continue.[197] As previously mentioned above, *Katz* established that a search could occur without physically entering a house or residence.[198] This definition is relevant today because it may allow police officers and other authorities the ability to access data stored by the Amazon Echo.[199] By obtaining data from an Echo device, authorities would be able to conduct a twenty-first century search of sorts, all without

[193] *See* Sitek, *supra* note 92 (summarizing how Bates consented to having Amazon release the data collected from his Echo device to government authorities); *see also* McLaughlin *supra* note 95 (reiterating on Bates' decision to allow Amazon to provide authorities with his Echo data).

[194] *See* Heater, *supra* note 97 (explaining that although Amazon refused to turn over Bates' Echo data and his attorney believed that it was a clear invasion of his privacy at home, Bentonville Police looked to the town utilities departments for further evidence).

[195] *See* Heater, *supra* note 97 (concluding that despite the fact that the issue over Bates' data did not reach court, and technology companies seek to protect their private information, it is likely that in the future similar cases will reach court and subsequently be litigated over).

[196] *See* Heater, *supra* note 97 (questioning the degree to which one's personal information from within the home is truly protected in a court of law); *see also* Wang, *supra* note 95 (suggesting that technology companies will want to litigate when the government seeks to infringe upon their private data).

[197] *See* Riley, *supra* note 76, at 2493 (suggesting that technological developments will force authorities to begin to investigate in unprecedented manners).

[198] *See* Katz, *supra* note 29, at 353 (reiterating a previously made point that the *Katz* case established not only that the Fourth Amendment protects people instead of places, but also that a search can occur without entering a building).

[199] *See* Sauer, *supra* note 8 (opining that authorities may be able to access the data stored on the Echo and similar devices because it is each companies' policy to store and use data obtained through inquiries).

stepping foot inside of a potential suspect's home.[200] Unlike in *Katz*, this type of search would not require a court to establish a new precedent such as the notion that the Fourth Amendment protects people, not places.[201] Instead, one can argue that the permission of such a search is merely a modern day development on the same idea.[202] Additionally, it is possible that future courts might further alter the findings of the *Katz* Court and rule that in the same respect that the Fourth Amendment protects people instead of places, it also protects people instead of specific items.[203] Although *Riley* states that officers must obtain a warrant prior to searching an item such as cellphone, the case proves that it is nonetheless possible for authorities to search smart devices.[204] There is no reason why such a trend would not continue with a smart home device such as an Echo.[205] It can be presumed that since a warrant would likely be necessary just to procure the physical device, authorities would also need to obtain a subsequent warrant to be able to search the content on the device.[206]

Such adaptation is evident in *Smith*, where the existence of the telephone forced the Supreme Court to make revolutionary decisions regarding phone usage and privacy.[207] Like in *Smith*, where the Supreme Court decided that dialed phone numbers did not receive Fourth Amendment protection because the numbers are willingly

---

[200] *See* Sauer, *supra* note 98 (comparing traditional searches with the changing nature of modernity's searches through the emergence of technological inventions and developments).

[201] *See* Katz, *supra* note 29, at 351 (presuming that while the next Amazon Echo case will be the first to determine the extent of device user's privacy, it will likely not require the attention of the Supreme Court).

[202] *See* Sauer, *supra* note 98 (presenting the idea that in the future when similar cases require authorities to search devices such as the Echo, it will only be the expansion of the traditional searches of yesteryear).

[203] *See* Katz, *supra* note 29, at 352 (elaborating that the Fourth Amendment protects people instead of physical locations).

[204] *See* Riley, *supra* note 76, at 2495 ("[O]ur answer to the question of what police must do before searching a cell phone seized incident to arrest is accordingly simple – get a warrant.").

[205] *See* Riley, *supra* note 76, at 2490 (discussing some of the capabilities of smartphones and similar devices such as the Echo).

[206] *See If These Walls Could Talk*, *supra* note 4, at 1941 (inferring that new devices such as the Echo will require law enforcement officers to obtain warrants to seize both the physical item as well as any digital data that exists within it).

[207] *See* Smith, *supra* note 37, at 752 (Marshall, J., dissenting) (providing insight as to what exactly occurred in the *Smith* case, and how authorities gained access to what was once believed to be private information).

exposed to third parties, it is very possible that a reviewing court will adopt this precedent for Amazon Echo inquiries.[208] Should this occur, it would seem that authorities would be able to successfully obtain such information that investigators coveted in the *Bates* case.

IV. Conclusion

Since the creation of the United States, a push to amend and alter its government has existed throughout the ranks of society. This effort has only been strengthened by societal developments in areas such as technology. Thanks to the tremendous degree of progress in the twentieth and twenty-first centuries, technology has evolved from having smart devices to now having smart homes. Nevertheless, the law has yet to evolve at the same rate as that of technology. Questions now exist as to how the law should address legal questions arising out of the smart home. Unfortunately, society will have to wait until the next smart home controversy arises before understanding how the law will address today's latest technology. Until then, it will have to rely on past cases to make the best predictions possible.

[208] *See* Smith, *supra* note 37, at 752 (leaving open the possibility of future litigation regarding the legitimate expectation of privacy using recordable devices).