4-26-2019

Alexa, Amazon Assistant or Government Informant?

Julia R. Shackleton Esq.

Alexa, Amazon Assistant or Government Informant?

Julia R. Shackleton, Esq.*

Alexa, are you listening to me? Technology has become an integral part of one's everyday life with voice-controlled devices pervading our most intimate interactions and spaces within the home. The answers to our questions are now at our fingertips with the simple roll of the tongue "Alexa," your very own personal intelligence assistant. This futuristic household tool can perform tasks that range from answering simple voice commands to ordering any online shopping. However, the advent of voice technology presents a myriad of problems. Concerns arise as these new devices live in the privacy of our homes while quietly listening for a "wake word" to record us—whether knowingly or unbeknownst to the owner or those nearby. This information is thereafter collected by Amazon and stored on its server.

Traditionally, the Fourth Amendment evolved through case law to provide citizens with protections when in the intimacy of one's home. Despite these protections, the third-party doctrine peels away a person's reasonable expectation of privacy when data or information is exposed to third parties.

* Julia R. Shackleton, Esq.; Judicial Law Clerk, Rhode Island Supreme Court; Staff Member, University of Miami Business Law Review, 2017-2018; University of Miami School of Law, Juris Doctor, 2018; Gettysburg College, Bachelor of Arts in Political Science, 2015. I would like to personally thank the Honorable Brian P. Stern, Special Assistant Attorney General Matthew L. LaMountain, and Deputy Clerk Carin B. Miley for their support and assistance throughout the research and writing process. I would also like to thank Professor Donald M. Jones for his immeasurable knowledge and guidance. Special thanks to the Editorial Board of the University of Miami Business Law Review for their hard work and diligence.

Thus, the question posed is whether there is any Fourth Amendment protection when information is digitally shared with other third parties, such as Amazon's Alexa? Further, what is even considered one's reasonable expectation of privacy in the modern digital world? Our generation is accustomed to surrendering a vast amount of personal and private information, particularly from current whereabouts through Facebook and Instagram check-ins and recent inquiries that are stored in search engine histories. This leaves an ascertainable digital trail to track where you have been, who your friends and family are, and even what you are thinking. How much of this digital information is obtainable by the government? Can this futuristic device—Amazon's Alexa—that we keep on our nightstands or kitchen tables actually be used against us?

Part I of this comment will present a series of murder cases that demonstrate the current legal stance of trial courts on this particular legal issue. Part II will describe how Alexa works and why Amazon would want to gather this information. Part III recapitulates the evolution of Fourth Amendment case law, particularly the privacy in a search, the admissibility for a man's private papers to be used as evidence against himself, and the sanctity of a man's home. Part IV discusses third-party doctrine case law and how this strips away all Fourth Amendment protections, and Part V analyzes the prior case law and proposes a modern application to the third-party doctrine.

I. INTRODUCTION

Technology has evolved at an unprecedented rate. Unfortunately, Fourth Amendment jurisprudence has not advanced at such great speed. The emergence of smart device technology has enabled us to live a life of ease, granting us accessibility to a mass amount of information and allowing us to always stay connected. Today, we can use a smart device to automate a text, surf the web, and to navigate to a location we have never been before. However, it is daunting that these devices are always tracking us and our search histories are saved as stored data by our providers and manufacturers.

A. Alexa, remind me to never ask you how to destroy evidence of murder

Richard Baribault, a man convicted of first degree murder, *inter alia*, is an exemplar of how invasive and incriminating smart devices can be.[1] In the early hours of the morning on August 1, 2015, a sailing nomad, affectionately known in the community as "Captain Fredy," was strangled to death on his boat in Warwick Cove Marina, Rhode Island.[2] Captain Fredy's body was not discovered until fifteen hot summer days later, after the body was almost unrecognizable due to its decomposition.[3] As

---

1 Ethan Hartley, *Baribault found guilty in murder of Capt. Fredy*, WARWICK BEACON (Jul. 5, 2017 12:45 PM), http://warwickonline.com/stories/baribault-found-guilty-in-murder-ofcapt-fredy,125784.

2 *Id.*

3 *Id.*

Warwick Police investigated the scene, the only telling evidence was motion-sensor video surveillance that, when activated, captured random moments during the murder and post clean-up.[4] However, due to the boat's far distance from the camera and the distortion of the image, the murderer was unascertainable.[5]

As Warwick Police interviewed Captain Fredy's marina neighbors, the investigators accrued a litany of individuals whom might have information about the murder.[6] Among those individuals was Richard Baribault. As law enforcement began interviewing Baribault,[7] they asked for Baribault's consent to search his phone.[8] The phone extraction revealed that Baribault had a Google application on his phone.[9] The extraction also provided the password to Baribault's Google account.[10] The detectives then logged into Baribault's account from a separate computer, which rendered access to his account.[11] The detectives listened to Baribault's automated recordings of his google searches and were able to identify his voice. His inquiries were as follows:

> On August 3, 2015 at 7:56 am – Does bleach kill everything including skin cells?
>
> On August 3, 2015 at 8:11 am – Boat moto mechanic in Warwick, Rhode Island?
>
> On August 6, 2015 at 12:14 pm – What towns have garbage days Friday morning?
>
> On August 6, 2015 at 12:14 pm – What towns in Rhode Island have garbage days garbage pickup Friday morning?
>
> On August 8, 2015 at 4:09 pm – Where would Warwick Harbormaster take a towed boat?[12]

---

4 *Id.*

5 *See id.*

6 Warwick Police Department Incident Report #15-3829-OF.

7 Of note, Law Enforcement in Rhode Island is not required to obtain a warrant to seize such information. However, it is common practice for the police force to obtain a warrant. Likewise, the Attorney General's office of Rhode Island also engages in same practice. Moreover, each state has its own standard protocol, but this requirement is not compelled by any form of legal precedent.

8 Warwick Police Department Incident Report #15-3829-OF.

9 *Id*.

10 *Id.*

11 *Id.*

12 *Id.*

Thereafter, the police obtained a search warrant to acquire from his provider his cell phone data—such as, call records, location data, and other cell phone content.[13] Baribault's cell phone, like all cell phones, was tracking his location at every second and could show his location based on the coordinates that the closest cell tower was tracking.[14] Ultimately, the location information provided the most incriminating evidence as Baribault's location matched the location and the time that the video surveillance activated during the time of the murder and post clean-up.[15]

However, the voice recordings of the previously listed inquiries were played during his trial and, most likely, had one of the greatest impacts on the jury. Without this information from Baribault's smart device, there may have never been enough information to track him and solve this murder. Yet, finding the murderer was at the expense of his own privacy. Indeed, Baribault consented to search his phone, but it is unclear if Baribault was fully aware of the information he surrendered to the police—GPS location tracking his every second, search engine history, and overly incriminating voice recording inquiries. The other question this case raises is whether the reasonable person is aware that information, such as the location that is tracked every second, is stored information that is obtainable by the government. Moreover, information that can be obtained even without a warrant in some jurisdictions.

B. Subpoena power over Amazon's Alexa records.

In another murder case, *State v. Bates*, officers from the Bentonville, Arkansas, Police Department were placed in a similar situation—an unsolved murder case coupled with smart home technology located at the scene of the crime.[16] As detectives investigated the murder, they found an Amazon Echo Dot.[17] After the discovery of the Amazon Echo, law enforcement seized the Echo and subpoenaed Amazon, claiming there was reason to believe Amazon.com was in possession of records associated with the homicide.[18]

---

13 Ethan Hartley, *Baribault found guilty in murder of Capt. Fredy*, WARWICK BEACON (Jul. 5, 2017 12:45 PM), http://warwickonline.com/stories/baribault-found-guilty-in-murder-ofcapt-fredy,125784.

14 *See id.*

15 *State of Rhode Island v. Richard Baribault*, K1-2016-0069B

16 *See generally* Complaint, State v. Bates, 2016 WL 7587405 (Ark. Cir. Aug. 26, 2016) (No. CR20160370).

17 Amy B. Wang, *Police Land Amazon Echo Data in Quest to Solve Murder*, CHICAGO TRIBUNE (March 9, 2017, 11:08 AM), http://www.chicagotribune.com/bluesky/technology/ct-amazon-echo-murder-wp-bsi-20170309-story.html.

18 *Id.*

Law Enforcement demanded records of the Amazon Echo device, alleging that the Amazon Echo stored recorded statements that would contain highly probative evidence of the incident—specifically, evidence that would discredit Bates' alibi. Additionally, Bates' water meter revealed that a substantial amount of water was used right after the murder was suspected to occur.[19] This led investigators to believe the patio and hot tub was hosed down prior to the arrival of the police.[20] Additionally, investigators learned that music was being played on the back patio at the time of Collin's death that could have been played by Amazon's personal intelligence assistant, Alexa.[21]

Amazon initially opposed the warrant, claiming that the police department did not affirmatively establish that their investigation outweighs the customer's privacy rights.[22] Specifically, Amazon stated, the company "will not release customer information without a valid and binding legal demand properly served on us."[23] The Brenton County prosecutor moved to compel Amazon to provide the data that Bates' Echo may have collected.[24] According to court documents, Bates' attorney did not object to the motion and agreed that Bates would voluntarily provide opposing counsel with the data collected.[25] Later that day, Amazon delivered the data per the customer's consent.[26]

Although Bates voluntarily consented to the production of the Amazon Echo records, this personal device that records our mental impressions and inquiries, overheard conversations, and other unknown statements is attainable information that the government can seize and use against us under the third-party doctrine. Nonetheless, most people in

---

19 Nicole Chavez, *Arkansas Judge Drops Murder Charge in Amazon Echo Case*, CNN (December 2, 2017, 12:52 AM), http://www.cnn.com/2017/11/30/us/amazon-echo-arkansas-murder-case-dismissed/index.html.

20 Eliott C. McLaughlin, *Suspect Oks Amazon to Hand Over Echo Recordings in Murder Case*, CNN (April 26, 2017, 2:52 PM), http://www.cnn.com/2017/03/07/tech/amazon-echo-alexa-bentonville-arkansas-murder-case/; *see also* Eliott C. McLaughlin & Keith Allen, *Alexa Can You Help with This Murder Case?* CNN (December 28, 2016, 8:48 PM), https://www.cnn.com/2016/12/28/tech/amazon-echo-alexa-bentonville-arkansas-murder-case-trnd/index.html.

21 McLaughlin, *supra* note 20.

22 *Id.*

23 Colin Dwyer, *Arkansas Prosecutors Drop Murder Case That Hinged on Evidence From Amazon Echo*, NPR (November 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 (citing *Arkansas Judge Drops Murder Charge in Amazon Echo*, AP NEWS (November 29, 2017), https://apnews.com/f66ee9c4e2514d4789a50324860a9c29).

24 *Id.*

25 *Id.*

26 *Id.*

society are oblivious to the third-party doctrine and the accessibility the government has over our private matters. Therefore, consumers are often uncertain of what privacy protections apply when it involves this extremely invasive technology that lives in the presence of one's home. Amazon's Alexa recordings have a similar nature to the traditional wiretap, however; Alexa's ability to answer any and all of our questions reveals a greater deal of information than a mere recording from a microphone. It reveals our questions, mental processes, and inner thoughts that ultimately reflect a wealth of information concerning a person's familial, political, professional, and religious affiliations.

Arguably, this information demands greater privacy protections than the home. However, the Fourth Amendment fails to provide the adequate privacy protection for smart technology devices. Justice Scalia in *Kyllo v. United States* proclaimed that "*all* details [in the home] are intimate details, because the entire area is held safe from prying government eyes."[27] Yet, Amazon's Alexa—a personal effect within the home—does not receive such protection. In light of the advancement of technology, the Court may have to reconsider Fourth Amendment jurisprudence in order to afford society with its reasonable expectation of privacy when using these invasive digital devices, especially in the sanctity of one's home.

C. What does Amazon do with all of this stored data?

Although Alexa provides convenience to its users, it undermines and diminishes one's privacy through its third-party interconnectivity. In order to get full use out of Alexa's skills, the user will ask Alexa's queries or commands. Alexa's responses are answered through her connection to third-party services, such as, but not limited to, other smart home devices, apps, or any website that Alexa accesses. The information that each user provides to Alexa is also voluntarily given to every other third party that Alexa uses in order to answer the query or command.[28] However, unbeknownst to most Alexa users, every Alexa owner entered into an agreement with Amazon's Digital Services LLC before they even used Amazon's Alexa.[29] This agreement renders all information to Amazon and other third-party users when using this smart device. Amazon even promotes that, "Alexa is Amazon's cloud-based voice service available on

---

27 533 U.S. 27, 37 (2001) (alteration in original).

28 *Why Alexa?*, AMAZON, https://developer.amazon.com/alexa (last visited January 26, 2018).

29 *Alexa Terms of Use*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=201809740, (last visited January 26, 2018).

tens of millions of devices from Amazon and third-party device manufacturers."[30]

Alexa is controlled by the voice of each user.[31] During the user's voice interactions, Alexa streams the audio to the Amazon cloud.[32] Amazon then processes and retains each user's voice command or query in the Amazon server,[33] including your voice inputs, music playlists, Alexa's to-dos, and shopping lists.[34] Moreover, this information is also transmitted to the third-party service or auxiliary product that is related to the command or quest.[35]

In the Alexa terms of use agreement, Amazon informs the reader that Amazon may exchange related information to a third-party service.[36] For instance, if a user simply asks, "Alexa, what is the weather like today?" Amazon will relay your current zip code to the third party weather service it uses to answer your query.[37] Although this example seems minor in scale, further use of Alexa creates an outgrowth of information that is given to other third-party networks and all networks that the third party associates with.[38] Amazon warns those who even bother to read its terms and use agreement that, "[y]our use of any Third Party Service is subject to this Agreement and any third party terms applicable to such Third Party Service . . . [i]f you do not accept the third party terms applicable to a Third Party Service, do not use that Third Party Service."[39]

However, the issue is that most of Alexa's owners have not even read Alexa's Terms of Use Agreement, let alone know that Alexa's interconnection activity subjects them to other companies' conditional Use of Terms Agreements. Every time a person uses Alexa, they are disclosing information, which inevitably turns into a treasure trove of information that has the possibility to circulate to public websites or allows for government tracking.[40] Furthermore, Amazon's Terms of Use Agreement specifically states, "[w]hen using a Third Party Service, you are responsible for any information you provide to the third party. Amazon has no responsibility or liability for Third Party Services. Publishers of

---

30 AMAZON, *supra* note 28.
31 AMAZON, *supra* note 29.
32 *Id.*
33 *Id.*
34 *Id.*
35 *Id.*
36 *Id.*
37 *Id.*
38 Steven I. Friedland, *Drinking from the Fire Hose: How Massive Self-Surveillance from the Internet of Things is Changing the Face of Privacy*, 119 W. VA. L. REV. 891, 897 (2017).
39 AMAZON, *supra* note 29.
40 Friedland, *supra* note 38, at 392.

Third Party Services may change or discontinue the functionality or features of their Third Party Service."[41]

II. FOURTH AMENDMENT JURISPRUDENCE

The Fourth Amendment declares, it is "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures . . . "[42] The Fourth Amendment implements constitutional limits on law enforcement's authority to conduct a "search" or "seizure."[43] A "search" transpires when: (1) the intrusion constitutes a common law physical trespass and invades a "constitutionally protected area"[44] within the bounds of the Fourth Amendment;[45] (2) for the purpose of obtaining information or attempting to find something;[46] and (3) the reasonable expectation privacy test survives despite a lack of physical trespass.[47]

Fourth Amendment protections have evolved from those originally grounded in notions of physical trespass.[48] Over time, the pendulum began to swing away from property notions and towards a more individualistic approach, which sought to protect the person, not the place.[49] The transformation of the Fourth Amendment's underlying rationale was largely due to the advances in technological development.[50] It was not necessarily the physical intrusion itself that violated the Fourth Amendment, but rather whether a person manifested a subjective expectation of privacy in the object of the challenged search and whether society was willing to recognize that expectation of privacy as reasonable.[51] However, under Fourth Amendment jurisprudence, there is no reasonable expectation of privacy in information voluntarily disclosed to third parties.[52] This note will analyze the Fourth Amendment protection

---

41 AMAZON, *supra* note 29.

42 U.S. CONST. amend. IV.

43 Riley v. California, 134 S. Ct. 2473, 2492 (2014).

44 "Constitutionally protected areas" includes places such as one's person, houses, papers, and effects. U.S. CONST. amend. IV.

45 Berger v. New York, 388 U.S. 41, 78 (1967) (Black, J. dissenting); *see also* United States v. Jones, 565 U.S. 400 (2012).

46 Clark D. Cunningham, *A Linguistic Analysis of the Meanings of "Search" in the Fourth Amendment: A Search for Common Sense*, 73 IOWA L. REV. 541 (1988).

47 Katz v. United States, 389 U.S. 347, 353 (1967).

48 *See* Olmstead v. United States, 277 U.S 438 (1928).

49 *See generally Katz*, 389 U.S. at 347 (1967).

50 *Id.*

51 *Id.*

52 Smith v. Maryland, 442 U.S. 735, 744 (1979).

in light of the development of smart home devices, such as Amazon's Alexa.

A. The evolution of the Fourth Amendment: Have we lost sight of the purpose of an unreasonable search?

Throughout the course of Fourth Amendment jurisprudence, the United States Supreme Court has varied in its interpretation of what the Fourth Amendment protects. The original concept of a Fourth Amendment search was illustrated by the Court in *Olmstead v. United States* in 1928.[53] The petitioners in *Olmstead* were convicted in the District Court for the Western District of Washington for conspiring to violate the National Prohibition Act by unlawfully possessing, transporting and importing intoxicating liquors and maintaining nuisances, and by selling intoxicating liquors.[54]

The information that led to the discovery of the conspiracy, along with its nature and extent, was obtained by intercepting telephone conversations of the conspirators by a federal officer.[55] The interceptions occurred from small wires that were inserted along the outside telephone wires from the residences of the petitioners and those leading from their office.[56] The insertions were made without trespassing on the petitioners' property, as the wiretapping insertions were affixed on public streets close to the petitioners' homes.[57] The Court found that there was no search under the Fourth Amendment because the electronic eavesdropping occurred without physical intrusion.[58] The crux of Justice Taft's analysis hinged on the inquiry of whether the underlying action by the federal officers happened inside the home.[59] Thus, because the evidence seized was not obtained by physical intrusion into one's home, but rather obtained only though hearing—no Fourth Amendment violation occurred.[60] At this time, the analysis of the Fourth Amendment search inquired into whether there was physical intrusion on one's property; thus, the Fourth Amendment protected property, not the person.

The precedent set forth by the *Olmstead* Court was later overruled in *Katz v. United States* in 1967.[61] The petitioner in *Katz* was convicted in the District Court for the Southern District of California for transmitting

---

53 *See generally Olmstead*, 277 U.S. at 438.
54 *Id.* at 455.
55 *Id.* at 456.
56 *Id.* at 456–57.
57 *Id.* at 457.
58 *Id.* at 464.
59 Olmstead v. United States, 277 U.S 438, 464 (1928).
60 *Id.*
61 Katz v. United States, 389 U.S. 347, 353 (1967).

wagering information by telephone from Los Angeles to Miami and Boston in violation of a federal statute.[62] During trial, the Government was allowed to introduce evidence that the petitioner objected to on grounds of violation of his Fourth Amendment rights.[63] Specifically, the evidence in question involved federal agents attaching an electronic listening and recording device to the outside of a public telephone booth, which the petitioner placed his calls from.[64] The *Katz* Court renounced the underpinnings of the *Olmstead* Court and held that physical trespass is no longer the controlling law under the Fourth Amendment.[65] The *Katz* Court noted that the Government's actions—electronically listening and recording the petitioner's conversation—violated the privacy upon which he "justifiably relied while using the telephone booth. Such actions constituted a 'search and seizure' within the meaning of the Fourth Amendment."[66] Importantly, the Court asserted that there was no constitutional significance to the fact that the electronic device did not penetrate or physically invade the phone booth.[67]

Justice Harlan, writing a separate concurring opinion in *Katz*, set forth a two-prong test, which the Supreme Court later endorsed in *Bond v. United States*.[68] Determining whether a search is reasonable requires: (1) the person to have manifested an actual subjective expectation of privacy; and (2) this expectation is one that society is prepared to recognize as reasonable.[69] Concerning the first prong of this test, Justice Harlan emphasized how one's personal aspect of privacy and their own subjective expectations of privacy can be inferred from their conduct.[70] Regarding the facts of *Katz*, Justice Harlan found it significant that the petitioner shut the door behind him when using the phone booth, thus demonstrating his expectation that his conversation will be private.[71] The *Katz* framework changed the analysis of whether a search is reasonable to focus on the subjective expectation of privacy. This shifts away from the past emphasis of property notions. The *Katz* Court found that the petitioner did in fact manifest a subjective expectation of privacy as he entered the phone booth in an attempt to exclude the "uninvited ear."[72]

---

62 *Id.*
63 *Id.*
64 *Id.* at 348.
65 *Id.* at 353.
66 *Id.*
67 *Id.*
68 *See* Bond v. United States, 529 U.S. 334, 338 (2000).
69 *Katz*, 389 U.S. at 361 (Harlan, J., concurring).
70 *Id.*
71 *Id.*
72 *Id.* at 352.

However, the notions of physical intrusion may have been resurrected in *United States v. Jones*.[73] The United States Supreme Court found that the government conducted an unlawful search when federal agents placed a GPS tracking device on the car of the respondent, which tracked the movements of the respondent over the course of 28 days.[74] The respondent filed a motion to suppress the evidence gained from the GPS, as the information collected not only his movements on public streets, but also when his vehicle was parked inside the garage of the home. In the majority opinion, Justice Scalia revived the property notion of an unreasonable search by stating, "as we have discussed, the *Katz* reasonable-expectation-of-privacy test has been *added to,* not *substituted for,* the common-law trespassory test."[75]

Although this case was ultimately decided on trespass notions, Justice Sotomayor notified the Court in her concurrence about the detrimental effects of the property-based test in the future.[76] Sotomayor opined that, due to the surge in use of technology, this test potentially chills one's associational and expressive freedoms.[77] Significantly, this is imperative when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements.[78] Sotomayor additionally foretold the privacy concerns as it relates to Amazon's Alexa and the third-party doctrine:

> More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers.[79]

Justice Sotomayor notably indicated that the third-party doctrine needs to be reexamined, particularly as we enter this new world of digital

---

73 565 U.S. 400 (2012).
74 *Id.* at 402.
75 *Id.* at 409.
76 *Id.* at 414.
77 *Id.* at 416.
78 *Id.*
79 *Id.* at 417.

technology that possesses the power of retrieving detailed information, such as what we are thinking, who are we intimately involved with, or where we are located. In light of the third-party doctrine's broad power, an officer can circumvent a warrant through subpoenaing information of third-party service parties. Thus, this doctrine not only enables law enforcement to arbitrarily exercise police surveillance, it encourages it.

B. Privacy within the home: Kyllo's impact

As noted above, Amazon's Alexa is commonly found within the owner's home, either in one's kitchen, living room, or nightstand. This presents a problem because the personal assistant is kept within the intimacy of one's home: Does the third-party doctrine penetrate through one's home and allow for the government to seize data containing conversations, sometimes conversations that were unknowingly recorded? Moreover, these personal assistants, which are pervading into everyday life through the use of other smart home technologies, can be used as surveillance tools in order to investigate any individual. Typically, courts have honored the home and what occurs therein, holding it is an intimate place of privacy under the Fourth Amendment.

In *Kyllo v. United States*, the Supreme court determined whether the use of a thermal-imaging device aimed at a private home from a public street to detect relative amounts of heat within a home constitutes a search under the Fourth Amendment.[80] The Court persisted with, "'[i]t would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology.'"[81] Ultimately, the Court found that the information regarding the interior of the home that could not have been obtained without physical intrusion into a constitutionally protected area constitutes a search—and especially so when the technology in question is not in general public use.[82] The Court reasoned that accepting the information attained by the thermal-imaging device would "leave the homeowner at the mercy of advancing technology . . . that could discern all human activity in the home."[83] Specifically, the Court described the intimate details advancing technologies could pick up, "for example, at what hour each night the lady of the house takes her daily sauna and bath—a detail that many would consider 'intimate'; and a much more sophisticated system detect nothing more intimate than the fact that someone left a closet light on."[84]

---

80 533 U.S. 27, 30 (2001).
81 *Id.* at 33.
82 *Id.* at 34.
83 *Id.* at 35–36.
84 *Id.* at 38.

Interestingly, this is exactly the issue with advancing technologies, like Alexa, and the government's ability to search troves of data controlled by companies, like Amazon. Now, under the third-party doctrine, an officer does not even need to bother with obtaining a search warrant and searching the house because the law already allows the government to search the data of any third-party service. Particularly with Alexa though, intimate details are potentially traceable from this personal assistant. For instance, the device could accidentally awake and record a vehement discussion between husband and wife.

Conversely, the *Kyllo* Court also stated, "the Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares." In relation to personal assistant devices, alternatively, an individual does voluntarily welcome these technologies into their home. Thus, under their own assumption of risk, they are arguably accountable for any consequences that pursue.

C. Privacy in one's private papers

Prior to the inception of the third-party doctrine, the United States Supreme Court decided that it was a violation of the Fourth Amendment to compel an individual to produce his or her own private papers.[85] In *Boyd*, several cases of glass were confiscated from the defendants pursuant to customs revenue law.[86] Thereafter, the district attorney subpoenaed the defendants to produce invoices concerning the seized plates of glass. [87] However, the defendants raised the question of whether it was constitutional under the Fourth Amendment to compel the defendants to produce private papers that could be used as evidence against him for the purposes of an unreasonable search and seizure within the Fourth Amendment.[88]

The *Boyd* Court held that the Fourth Amendment protects against the invasion into a person's private matters and will not allow the government to compel a person to produce private papers.[89] The Court delved into the history and reasoning behind the Fourth Amendment unreasonable search and seizures, specifically the issuance of the writs of assistance.[90] The practice enabled revenue officers to issue writs of assistance, which empowered them to use arbitrary and sole discretion to search suspected

---

85 Boyd v. United States, 116 U.S. 616 (1886).
86 *Id.* at 617.
87 *Id.*
88 *See id.* at 619.
89 *Id.* at 624.
90 *Id.* at 625.

places for smuggled goods. James Otis pronounced it was the "worst instrument of arbitrary power, the most destructive of English liberty and the fundamental principles of law, that ever was found in an English law book . . . [because] the liberty of every man [was placed] in the hands of every petty officer."[91] The writs of assistance authorized customs officers to enter and inspect houses without any warrant.[92] Moreover, customs officers could obtain a writs of assistance without even alleging any illegal activity that would precondition the search.[93] The *Boyd* Court noted that it was the writ of assistance that inaugurated the resistance of the colonies against Great Britain, which ultimately led to the Fourth Amendment's unreasonable searches and seizures.[94] The Court further noted that the Fourth Amendment applies to all invasions on the part of the government involving the sanctity of a man's home and the privacies of his life.[95]

Notably, the Court indicated that is it not the physical trespass, such as rummaging through a person's drawers, that constitutes an unreasonable search.[96] However, it is "the invasion of his indefeasible right of personal security, personal liberty, and private property, where that right has never been forfeited by his conviction of some public offense."[97] This notion of personal liberty aligns with the underlying premise of *Katz*, which endorses the concept that the Fourth Amendment protects the person, not the place.[98]

Specifically pertaining to the facts surrounding *Boyd*, it is the forcible and compulsory extortion of a man's own testimony through his private papers—used as evidence against him—that contradicts the Fourth and Fifth Amendments.[99] The Court reasoned that the compulsory production of a man's private paper to be used in evidence against him is equivalent to compelling him to be a witness against himself in contradiction of the Fifth Amendment.[100] In light of the Fourth Amendment, the compulsory

---

91 *Id.* (quoting Cooley, Const. Lim. 301–303; John Adams, vol. 2, Appendix A, pp. 523–525; vol. 10, pp. 183, 233, 244, 256, etc., and in Quincy's Reports, pp. 469–482; and see Paxton's Case, Id. 51–57).

92 *See generally* William J. Cuddihy, *The Fourth Amendment: Origins and Original Meaning*, 602-1791, at 758–59 (1990) (unpublished Ph.D. dissertation, Claremont Graduate School) (available from UMI Dissertation Services, 300 N. Zeeb Road, Ann Arbor, Michigan).

93 *Id.* at 762–63.

94 *See Boyd*, 116 U.S. at 627.

95 *Id.* at 630.

96 *Id.*

97 *Id.*

98 *Compare* Katz v. United States, 389 U.S. 347, 368 (1967), *with Boyd*, 116 U.S. 630.

99 *See generally Boyd*, 116 U.S. 630.

100 *Id.* at 633.

production that coerces an individual to turn over their private papers constitutes an unreasonable search and seizure.[101]

III. THE GROWTH AND CURRENT APPLICATION OF THE THIRD-PARTY DOCTRINE

Under the third-party doctrine, an individual does not have a reasonable expectation of privacy regarding the information that he or she voluntarily disclosed to a third-party.[102] This doctrine initiated in the 1970's and was solidified by *Smith v. Maryland* in 1979.[103] Currently, the application of the third-party doctrine strips an individual of his or her Fourth Amendment protection, which allows the government to access information rendered to a third party without a warrant.[104] Although at first glance this case law precedent may not seem alarming, modern technology requires an individual to surrender a digital trail of their daily life in order to participate in our technological world. Knowing the government can access this information without a warrant leaves the masses uneasy.

Almost all of our personal information is disclosed to a third-party service provider. For instance, our personal and intimate text message conversations between our significant other or close friends; our e-mails to our superiors regarding potentially privileged work matters; our credit card statements and banking transactions; and our check-ins through Facebook and Instagram all reveal a wealth of information about our personal lives without any form of protection. Under the *Katz* test, the standard remains that the reasonable person must have a legitimate expectation of privacy in the activity that is searched for purposes of the Fourth Amendment.[105] But, is it that the average person in today's world does not value their right to privacy by constantly sharing intimate details about their life through Snapchat and other third-party service providers? Or is it that the right to privacy is no longer existent for those who participate in this digital world?

---

101 *Id.* at 622.

102 Note, *If These Walls Could Talk: The Smart Home and The Fourth Amendment Limits of The Third Party Doctrine*, 130 HARV. L. REV. 1924 (2017).

103 *See* United States v. Couch, 409 U.S. 322 (1973); *see also* Smith v. Maryland, 442 U.S. 735 (1979).

104 *See* Orin S. Kerr, *The Case for the Third Party Doctrine,* 107 MICH. L. REV. 561, 563 (2009) (defining the third party doctrine).

105 *Katz*, 389 U.S. at 361.

A. Origination of the third-party doctrine: Couch v. United States

After the establishment of the reasonable expectation test in *Katz*, the Court was faced with the question of whether the Fourth Amendment protects information conveyed to a third party. The third-party doctrine originated in *Couch v. United States* in 1973.[106] After the petitioner was suspected for a potential tax liability, the Government summoned the petitioner's accountant to provide all records, bank statements, cancelled checks, workpapers, and other pertinent documents pertaining to the tax liability of the petitioner.[107] The petitioner raised the argument that the confidential nature of the accountant-client relationship and, consequently, her expectation of privacy that existed when she handed over her private records protects her under the Fourth and Fifth Amendment from their production.[108] The Court found that the accountant-client privilege does not exist under federal law and, furthermore, no state-created privilege has been acknowledged in federal cases.[109]

The *Couch* Court continued and addressed the Fourth Amendment precedent set forth in *Boyd* concerning an individual's private papers.[110] The Court noted that there is a minimal expectation of privacy where records are voluntarily given to an accountant while under the understanding that mandatory disclosure is required for an income tax return.[111] Furthermore, the information disclosed was in the possession of the third-party service, the accountant, not the petitioner.[112] Therefore, the petitioner cannot reasonably claim Fourth Amendment protection for the purposes of privacy.[113] The *Couch* Court also addressed the argument that the Fifth Amendment protects compulsory production of the petitioner's documents because it is a form of self-incrimination.[114] However, the Court reasoned that the privilege against self-incrimination is an intimate and personal one, which defers to a private inner sanctum of individual feeling and thought, not to information that may incriminate an individual.[115] Ultimately, under the *Couch* ruling, personal information

---

106 409 U.S. 322 (1973).
107 *Id.* at 323.
108 *Id.* at 335.
109 *Id.*; *see also* Falsone v. United States, 205 F.2d 459, 463–64 (6th Cir. 1951); *see also* Himmelfarb v. United States, 175 F.2d 924, 939 (9th Cir. 1949).
110 *Couch*, 409 U.S. at 335.
111 *Id.*
112 *Id.*
113 *Id.*
114 *Id.* at 323.
115 *Id.* at 328. (quoting Justice Holmes "a party is privileged from producing the evidence, but not from its production.") (citing Johnson v. United States, 228 U.S. 457, 458 (1913)).

that is voluntarily given to a third party renders an individual with no expectation of privacy, which is daunting precedent considering today's digital world in which mass amounts of information are transmitted by third-party service providers.[116]

B. Banking statements: private papers that are protected?

The Court again addressed the question of the third-party doctrine in *United States v. Miller*, where the government accessed the suspect's banking statements and records—without a warrant.[117] The *Miller* Court denied the defendant's motion to suppress subpoenaed banking documents because the Court found there was no legitimate Fourth Amendment interest that was implicated by the government's investigation; specifically, there was no governmental intrusion into a constitutionally protected zone of privacy that the defendant relied on.[118] The *Miller* Court highlighted the *Katz* expectation of privacy test and quoted, "in *Katz* the Court also stressed 'what a person knowingly exposes to the public . . . is not subject of Fourth Amendment protection.'"

Thus, it reaffirmed that information conveyed to a third-party service provider is not warranted Fourth Amendment protection. The Court distinguished the subpoenaed banking records from the documents in *Boyd*, indicating that the banking statements and records here do not constitute "private papers."[119] Rather, the documents consist of business records that belong to the bank; therefore, the defendant cannot assert ownership nor possession on the claim for an illegal seizure.[120] The Court specifically stated,

> The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[121]

---

116 Note, *supra* note 102, at 1929.
117 425 U.S. 435, 437 (1976).
118 *Id.* at 440.
119 *Id.*
120 *Id.* at 442.
121 *Id.* at 443 (citing United States v. White, 401 U.S. 745, 751-52 (1971); Hoffa v. United States, 385 U.S. 293, 300 (1966); Lopez v. United States, 373 U.S. 427 (1963)).

Therefore, what actually is a person's reasonable expectation in a world where, in order to subsist, one *must* rely on other third-party service providers to maintain a job, pay taxes, and communicate with friends and family?

Although the defendant in *Miller* did voluntarily and knowingly transact with the bank, it is imperative to note that the documents requested in *Miller* are the functional equivalent of the private papers compelled in *Boyd*. The private papers in *Boyd* were invoices constituting the sale or record of the fraudulently purchased glass.[122]Alternatively, the documents in *Miller* consisted of deposit slips and copies of checks.[123] Both documents comprise of sale transactions; however, the compelled documents in *Miller* involved a third party. Arguably, the main difference is caused by the modernization and accessibility of banking. Today, an individual can remotely deposit a personal check online or through a picture on their mobile phone.[124] Additionally, restricted banking hours no longer exist due to the creation of ATM machines.[125] Indeed, the banking statements in *Miller* are not "private papers," but it is vital to note the evolution of modern technology subjects a person to have no Fourth Amendment protections under the current precedent of the third-party doctrine. Mainly, one must either surrender their Fourth Amendment right or the courts must conclude that today's digital world affects one's expectation of privacy.

C. No expectation of privacy in a pen register because people know of them

The United States Supreme Court solidified the third-party doctrine in *Smith v. Maryland*, where the Court suppressed bank records and found that the government's use of a pen register, a device that records the numbers dialed by a phone, did not constitute a search.[126] After the victim received a number of harassing phone calls, law enforcement placed a pen register on the defendant's telephone without a warrant.[127] The defendant queried whether the installation and use of the pen register by the

---

122 Boyd v. United States, 116 U.S. 616 (1886).

123 *Miller*, 425 U.S. at 437.

124 *How Do You Deposit a Check With your Smartphone or Tablet?* FDIC, https://www.fdic.gov/consumers/consumer/news/cnsum16/photos.html (last visited January 26, 2018).

125 Linda Rodriguez McRobbie, *The ATM is Dead. Long Live the ATM!* THE SMITHSONIAN (January 8, 2015), https://www.smithsonianmag.com/history/atm-dead-long-live-atm-180953838/.

126 442 U.S. 735 (1979).

127 *Id.* at 737.

telephone company at the request of law enforcement constituted an unreasonable search and seizure.[128]

The Court initiated its analysis with the application of the *Katz* test, affirming that the determination of an unreasonable search hinges on whether a person invoking its protection can claim a justifiable, reasonable, or legitimate expectation of privacy that was invaded by the government.[129] The Court then analyzed the nature of the activity that was investigated by the government when the device was installed.[130] In regards to an actual expectation of privacy, subscribers are aware that they must convey phone numbers to the telephone company in order to complete their phone calls.[131] Moreover, it is well known that phone companies must make permanent records of the numbers they dial in order to generate permanent billing records.[132] Pen registers are also a common use of practice by telephone companies for billing purposes.[133] However, "[while] most people may be oblivious to a pen register's esoteric functions, they presumably have some awareness of one common use."[134] The Court opined that this must be common knowledge since most phone books inform subscribers in "Consumer Information" that they have the ability to identify unwelcome and troublesome phone calls.[135]

The *Smith* Court also found there was no expectation of privacy in a dialed phone number because the pen register was installed on telephone company property at the telephone company's central offices. The Court found the defendant cannot claim that his property was invaded or that the police intruded in a constitutionally protected area.[136] Additionally, the Court noted that the information discovered by the pen register is minimal, such that they do not expose the substantive contents of the conversation between the caller and recipient.[137] Therefore, under *Smith's* precedent, an individual has no expectation of privacy from a warrantless government

---

128 *Id.* at 738.

129 *Id.* at 739; *see also* Rakas v. Illinois, 439 U.S. 128, 142 (1978); *id.* at 150-51 (concurring opinion); id. at 164 (dissenting opinion); *see also* United States v. Chadwick, 433 U.S. 1, 7 (1977); *see also* United States v. Miller, 425 U.S. 435, 442 (1976); *see also* United States v. Dionisio, 410 U.S. 1, 14 (1973); *see also* Couch v. United States, 409 U.S. 322, 335–36 (1973); *see also* United States v. White, 401 U.S. 745, 752 (1971) (plurality opinion); *see also* Mancusi v. DeForte, 392 U.S. 364, 368 (1968); *see also* Terry v. Ohio, 392 U.S. 1, 9 (1968).

130 *Smith*, 442 U.S. at 741.

131 *Id.* at 742.

132 *Id.*

133 *Id.* (citing *The Legal Constraints upon the Use of the Pen Register as a Law Enforcement Tool,* 60 CORNELL L. REV. 1028, 1029 (1975)).

134 *Id.*

135 *Id.* at 742–43.

136 *Id.* at 741.

137 *Id.*

investigation involving information that was voluntarily rendered to a third-party service provider.

However, Justice Stewart wrote a dissenting opinion finding that recorded dialed phone numbers is no different than an electronically transmitted conversation; thus, the information gathered in *Smith* should fall within the purview of the Fourth Amendment.[138] Notably, Justice Stewart illustrated that the *Katz* Court recognized the "[t]he role played by a private telephone is even more vital, and since *Katz* it has been abundantly clear that telephone conversations carried on by people *in their homes or offices* are fully protected by the Fourth and Fourteenth Amendments."[139] Moreover, it is evident through subsequent case law precedent that telephone conversations between a caller and recipient are provided Fourth Amendment protections.[140] The dissent recognized that the majority opinion rested its argument on the theory that the caller is aware the telephone number dialed is recorded by the telephone company, but the telephone conversation is also electronically transmitted by the telephone company and on its property.[141] This information should also be afforded protection by the Fourth Amendment because it is derived from the private conduct within the home or office.[142] Additionally, it is undisputed that an individual would not remain content if a list of their phone calls were publicly broadcasted to the world.[143] Not because this information is incriminating, but rather because it "could reveal the identities of the persons and the places called, and thus reveal the most intimate details of a person's life."[144]

Since *Smith v. Maryland* in 1979, the third-party doctrine has remained relatively untouched. Courts have applied the doctrine with relative uniformity, applying it to information disclosed to internet service providers,[145] cell site data,[146] bank records,[147] employment records,[148] and cell phone records.[149] However, this lodestar decision was issued over

---

138 *Id.* at 746.

139 *Id.* (quoting Katz v. United States, 389 U.S. 347, 352 (1967) (emphasis added)).

140 *Id.* (first citing United States v. United States District Court, 407 U.S. 297, 313 (1972); then citing *Katz*, 398 U.S. at 352).

141 *Id.*

142 *Id.* at 747. Although this case was decided before the boom of mobile phones, the application of Katz is possibly still applicable even to mobile phones if a person demonstrates conduct that shows they had an actual subjective expectation of privacy.

143 *Id.* at 748.

144 *Id.*

145 Guest v. Leis, 255 F.3d 325, 335–36 (6th Cir. 2001).

146 United States v. Guerrero, 786 F.3d 351, 359–61 (5th Cir. 2014).

147 United States v. Suarez-Blanca, No. 1:07-CR-0023, 2008 WL 4200156, at *8 (N.D. Ga. Apr. 21, 2008).

148 *Id.*

149 *Id.*

thirty years before the use of mobile phones, laptops, and most importantly, digital personal assistants. This doctrine is outdated.

IV. REASONABLE EXPECTATION OF PRIVACY IN AN INTERNET INFUSED WORLD

In a foregoing time, a person had control over their own information—personal documents of banking or business transactions existed on a sheet of paper that the person possessed in their file cabinets.[150] The scribbles and intimate handwritten notations in one's diary would be safely tucked away under their pillow or buried in their nightstand.[151] Letters from one's dearly loved ones written on parchment paper would be housed in their slant front desk.[152] All of one's papers and personal information were privately stored within the home. Importantly, if the government wanted to inquire about one's personal information, it was required under the Fourth Amendment for the government to obtain a warrant to search one's home.[153]

Now, in a world with ever-changing technology, the government can track a person through the use of data that is broadcasted on a massive scale without ever obtaining a warrant.[154] Under the third-party doctrine, if one's personal information is in the hands of a third-party service, even if unknowingly, there is no reasonable expectation of privacy.[155] Yes, there is absolutely no Fourth Amendment protection. But, how can that be? Does that mean the government can view my recent purchases made with my credit card? Yes, because that information is also in the hands of your bank. What about my text messages between my husband? Yes, because those text messages are shared with both your telephone provider and potentially the manufacturer of your phone. Could the government even see what I am movie I am streaming on my laptop? Yes, because Netflix or whichever service provider you are using has a record of it.

What information was once safely kept private and sound in the intimacy of our homes is now essentially public information that is easily accessible by the government. Moreover, this is no minimal amount of information that is easily accessible. It is infinite. "Consumer reporting agencies have data about where you live, your financial accounts, and your history of paying your debts. Hospitals and insurance companies have your

---

150 DANIEL J. SOLOVE, NOTHING TO HIDE 102 (Yale Univ. Print, 2011).
151 *Id.*
152 *Id.*
153 Olmstead v. United States, 277 U.S. 438 (1928).
154 Solove, *supra* note 150.
155 Smith v. Maryland, 442 U.S. 735, 744 (1979).

health data."[156] But wait, there is more. The information on your Instagram, the people you search on Facebook, the stories you send to your friends on Snapchat are available to the government. Currently, legal scholars have denounced the law of search and seizure as "embarrassing"[157] and "archaic."[158] The Fourth Amendment is struggling from both modern development in technology and the constitutional tension between formalists and realists.[159]

A. Does the Fourth Amendment still carry the same spirit after the inception of the third-party doctrine and invention of Alexa?

This Note began its Fourth Amendment analysis by delving into the origin of the Fourth Amendment search; specifically, how the Court defined a search and what dispositive factors queue to an unreasonable search. Importantly, Olmstead demonstrated that the Court, at that time, viewed an unreasonable search to transpire when there was a physical intrusion into one's home—ultimately protecting one's property, not the person. What is interesting about this test, in relation to Amazon's Alexa, is that Alexa is property belonging to the owner, which would require a physical trespass in order to obtain its data. Also, Alexa is commonly kept inside the owner's home, therefore, allowing law enforcement to enter into the home. The physical intrusion into the home could also stem from finding out whether the homeowner uses an Alexa through billing records, which would require law enforcement to obtain this data from other types of technology that are not used by the general public.

This is explicitly what Justice Taft's analysis hinged on—physical intrusion inside the home. Accordingly, under this test, the government's search of obtaining Alexa without a warrant, which is the current standing case law, would not pass muster under *Olmstead*. It was not until the revelation of the third-party doctrine that retrieving this information without a warrant was considered reasonable. But was that the traditional intentions of the framers when enacting the Fourth Amendment? Indeed, *Olmstead* was decided more than a century after the Fourth Amendment was enacted. Nonetheless, other Fourth Amendment precedent decided closer to the enactment also supports and urges that the third-party

---

156 Solove, *supra* note 150 at 102–03.

157 Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 757–59 (1994).

158 Norman M. Robertson, *Reason and the Fourth Amendment—the Burger Court and the Exclusionary Rule*, 46 FORDHAM L. REV. 139, 175 (1977).

159 TIMOTHY O. LEARY, PRIVACY IN THE DIGITAL AGE (Nancy S. Lind & Erik Rankin eds., 2015).

doctrine, as it pertains to Alexa, would not suffice under the original notions and purposes of the Fourth Amendment as evidenced in *Boyd*.

The principle of *Boyd v. United States* was for a person to be secure in their home without government intrusion into a person's private matters and personal papers. This holding was ultimately enforced to uphold the Fourth Amendment, which was enacted to prevent the common practice of writs of assistance. The framers were wary of these general warrants, as they granted revenue officers with arbitrary and sole discretion to search whomever without a warrant. Additionally, this included the right for an officer to even enter one's home and inspect it. Interestingly, the third-party doctrine grants the government with a very similar flavor of arbitrary and excessive discretion of the general warrants. The purpose of the Fourth Amendment was not to solely ban the use of general warrants in the customs context specifically, but it was to prohibit the idea and the exercise of such broad discretion, particularly when it had to deal with one's private papers or the home. Today, under the third-party doctrine, the government can engage in a similar practice that the Fourth Amendment and cases, such as *Boyd*, attempted to prevent from occurring.

Thus, the hard question posed is what should members of American society expect in regard to their third-party information, information they never knowingly consented to sharing? Have we as a society *knowingly* given up our reasonable expectation of privacy in information about us? If we did not, what can we do other than acquiesce after the fact? Although the government will argue that, under one's user agreement the company, can collect and use the data, but this is the equivalent of an adhesion contract.[160] Moreover, the data collected by Amazon's Alexa could be viewed as the modern-day private papers of an individual. It records our trail of thoughts and questions, which has similar characteristics to our mental notes that one would leave in their diary. Moreover, under the third-party doctrine, the government is legally allowed to obtain other personal information merely because the individual used a third-party service.

Notably, in today's world, an individual does not have much choice of using or not using these third-party services. For instance, one arguably needs to have an e-mail in today's world in order to obtain a job at any entry level. Or one needs to have a cellular phone in order to keep in contact with other members of society given today's mobile society where friends and family could live all over the world. Thus, given society's current accessibility to travel and ease of communication, it is almost expected of an individual to swiftly respond to an e-mail within minutes

---

160 JOHN WESLEY HALL, SEARCH AND SEIZURE n.2 (5th ed. 2013). An adhesion contract is a non-negotiable contract that no person has to the time to read due to its length.

or the hour. Moreover, most of one's daily tasks involves using a third-party service provider. For instance, most people today make their daily purchases through a card, not cash.[161] Also, getting the daily news is now commonly accessed online or through an app rather than receiving a newspaper. However, even if one still receives a particular newspaper, the purchase of that subscription requires a credit card. Therefore, in order to live in today's world, an individual's livelihood is at the mercy of third-party services.

B. We still have a reasonable expectation of privacy, but something needs to change

Nonetheless, there are two notable arguments to be made under the reasonable expectation of privacy. One argument relates to the liberty notion and personal autonym that was set forth in *Katz*. The second argument hinges on the property notion that Justice Scalia advocated for in *Jones*. Both are currently standing law and arguably equally applicable to determine whether a search is determined unreasonable. Moreover, Justice Sotomayor, in her concurrence in *Jones*, opined that determining whether a search is unreasonable is not only founded based on the property notion that the majority in *Jones* stated, but also determined on whether the government violates a subjective expectation of privacy.

The Liberty Notion

Under the liberty notion, *Katz* set forth that determining whether a search is reasonable requires the person: (1) to have manifested an actual subjective expectation of privacy; and (2) this expectation is one that society is prepared to recognize as reasonable.[162] In relation to using Amazon's Alexa, it is possible that the individual is unknowingly being recorded by the device. Thus, if a husband and a wife get into an argument in the privacy of their bedroom, and Alexa unknowingly turns on and begins to record, the couple arguably had a reasonable expectation of privacy with the unknown communication conveyed to Alexa. Factors involving this reasonable expectation of privacy would include that the couple decided to speak to one another within their home, within in their bedroom, and without their knowledge that Alexa recorded the conversation. Additionally, the couple could arguably make the point that that intimate conversation was never intended for the government to easily obtain.

---

[161] Ellen Sirull, *Cash v. Credit Cards: Which Do Americans Use Most?* EXPERIAN (June 18, 2018), https://www.experian.com/blogs/ask-experian/cash-vs-credit-cards-which-do-american-use-most/.

[162] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J. concurring).

Additionally, when considering the existence of a reasonable societal expectation of privacy, does the reasonable person know that all of this massive information is easily accessed information by the government? I would argue that most people are unaware that their bank accounts and text message conversations can be viewed without any compelling interest. As Justice Sotomayor eloquently queried, "I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."[163] Moreover, granting the government with so much power allows for arbitrary discretion and potential abuse. As it stands right now, the third-party doctrine enables the police to easily engage in police surveillance and monitoring of one's daily life.[164]

The Property Notion

A stronger argument can be made by virtue of the property notion set forth in *Jones*, which held that a physical trespass by the government constituted an unreasonable search and seizure. Similar to the car in *Jones*, a person's Alexa or Echo Dot is also their personal property that they possess. Moreover, similar to how the car in *Jones* was driven on public roads, the information shared to third parties is also public information. The *Jones* Court specifically rejected the government's contention that there is no reasonable expectation on public roads; similarly, Alexa is shared information with Amazon. A search by the government without a warrant, however, is a physical trespass on the owner's property, Alexa. Additionally, now with the ease of the digital world, law enforcement would not have to go through the extensive measures of even placing the tracking GPS on an automobile because, under the third-party doctrine, they can access our digital trail even without a warrant.

However, in regard to the third-party doctrine, it is time to reconsider one's reasonable expectation of privacy in this digital world. In *Jones*, Justice Sotomayor noted that the current third-party doctrine is ill suited to the digital age, where mass amounts of information are revealed by individuals to third parties.[165] Moreover, it needs to be reconsidered as it becomes harder to function in the political, economic and social world without sharing electronical data, which leaves the public with a dissatisfaction in the law. Arguably, information disclosed to third parties can be determined as protected for purposes of a search under either the physical trespass test in *Jones* or the liberty interest test in *Katz*.

---

163 United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J. concurring).
164 *Id.* at 417.
165 *Id.*

As Justice Stewart indicated in *Smith* in 1979, the majority of people would not remain content with having their personal information being publicly broadcasted.[166] Not because this information is incriminating, but rather because this information reveals one's personal and intimate life to all. This information reflects a wealth of detail concerning an individual's familial, professional, political, religious, and sexual associations. Through this information obtained by third-party service providers, it would not be difficult to discover whether a person visited a therapist, has gone to an abortion clinic, had an intimate relationship with a person of the same sex, had an affair, or recently visited a strip club. The government can search one's personal records that have been stored throughout one's lifetime. Thus, a doctrine that grants such unfettered discretion to law enforcement and the government has the ability to chill one's associational and expressive freedoms. Therefore, it is imperative for the Court to reconsider the third-party doctrine and use a narrower construction that would greatly limit the government's ability to obtain an individual's personal and private information.

V. CONCLUSION

The Framers of the Constitution strongly advocated for the Fourth Amendment to protect the privacy of their documents and papers with their mental impressions and beliefs, particularly after their discontent with the British invading individuals' privacy on the basis of using general warrants. Due to the broad use of the third-party doctrine, the government is granted similar general warrant power that the Fourth Amendment ultimately intended to prevent. Given that advancing technologies have created devices, such as Amazon's Alexa, that can record our mental impressions, queries, commands, and conversations, either knowingly or unbeknownst, it is necessary for the government to place a narrower construction on the third-party doctrine.

166 442 U.S. at 744.