Roger Williams University Law Review

Volume 25 | Issue 1 Article 7

Winter 2020

The Old Bailment Doctrine: The Answer to Fourth Amendment Jurisprudence in the Digital Age

Shane Gallant
Candidate for Juris Doctor, Roger Williams University School of Law,2020

Comments

The Old Bailment Doctrine: The Answer to Fourth Amendment Jurisprudence in the Digital Age

Shane Gallant*

INTRODUCTION

In today's digital world, private citizens are finding a certain level of satisfaction and reliability in all aspects of life. From self-driving automobiles to the newly integrated smart homes and cities—life could not be easier. For example, Tara is a business executive who is always on the go. To save time, she has outfitted her home with today's most innovative technology. She purchased an Amazon Echo that is powered by Amazon's voice-activated assistant, Alexa.[1] Tara uses this device to make purchases, place phone calls, send text messages, maintain her calendar, play music, and control the lights and home security system.[2] However, Tara

* Candidate for Juris Doctor, Roger Williams University School of Law, 2020. A special thank you to Professor Emily Sack for her guidance throughout the writing process. To my wife, Tara, thank you so much for supporting me throughout my law school career.

1. Ry Crist & Andrew Gebhart, *Everything You Need to Know About the Amazon Echo*, CNET (Sept. 21, 2018, 10:49 AM), https://www.cnet.com/how-to/amazon-echo-alexa-everything-you-need-to-know/ [https://perma.cc/4R7V-ECJC].

2. *Id.* In the United States, the Amazon Echo now features over 30,000 skills that help make everyday life easier. Bret Kinsella, *Amazon Alexa Skill Count Surpasses 30,000 in the U.S.*, VOICEBOT (Mar. 22, 2018, 4:57 PM),

likely does not know that each call, text, purchase, and request is stored and timestamped on Amazon's cloud.[3]

Today, lives are run through devices like cell phones, products such as the Amazon Echo, and social media platforms. Technological globalization has generated many legal questions, the most important of which deal with personal privacy. Assume, for example, the government suspects Tara of a crime. Through some quick investigating, the government determines that much of her personal information is stored on Amazon's cloud because many of Tara's electronic devices are connected to her Amazon Echo. The issue is that many people do not understand the extent to which the government can obtain data stored on a company's cloud service. The hard truth is that the government seldom needs a warrant to access one's sensitive information stored with a third party,[4] and those third parties will not always provide notice when the government is requesting said information.[5]

Like most people, Tara does not think of the privacy implications of the digital age; she is just happy to live in an advanced society, especially after her father's recent heart attack. Given advancements in medical technology, Tara's father, Bill, is comfortable knowing that he has a new pacemaker that allows for real-time wireless monitoring, an implantable cardioverter defibrillator, and long-lasting battery life that automatically transmits its data straight to his physician.[6] Bill's physicians have

---

https://voicebot.ai/2018/03/22/amazon-alexa-skill-count-surpasses-30000-u-s/ [https://perma.cc/9EEW-LHUE].

3. *See* Russel Brandom, *How Much Can Police Find Out from a Murderer's Echo?*, THE VERGE (Jan. 26, 2017, 9:05 AM), https://www.theverge.com/2017/1/6/14189384/amazon-echo-murder-evidence-surveillance-data [https://perma.cc/S9HZ-9JCB]. According to Amazon, "[C]loud storage is a cloud computing model that stores data on the Internet through a cloud computing provider who manages and operates data storage as a service." *See Cloud Storage*, AMAZON, https://aws.amazon.com/what-is-cloud-storage/ [https://perma.cc/X9PV-4QZZ] (last visited Sept. 29, 2019).

4. *See* Anne Pfeifle, Comment, *Alexa, What Should We Do About Privacy? Protecting Privacy for Users of Voice-Activated Devices*, 93 WASH. L. REV. 421, 430-31 (2018); *see also infra* Part IV.

5. *See* Pfeifle, *supra* note 4, at 431–32 ("Microsoft alleged that in a twenty-month period, federal courts issued 3,250 secrecy orders to Microsoft alone to prevent it from communicating with customers about requests for data, and of those about two-thirds had no end date.").

6. Dave Fornell, *New Pacemaker Technologies*, DAIC (Feb. 13, 2018), https://www.dicardiology.com/article/new-pacemaker-technologies [https://

all the recorded data at their disposal to make adjustments to his treatment as needed, which Bill loves since he no longer needs to make multiple trips to his doctor for testing. But, should Bill feel so comfortable? Could the government simply subpoena or obtain a court order for Bill's pacemaker information if they believed that he was connected to a crime? Sadly, for Tara and Bill, the government can obtain Tara's records from Amazon's cloud service as well as the pacemaker records from Bill's doctor through a court order or subpoena.[7] As society advances into a new technological era, current laws will continue to lose their effect in protecting a citizen's privacy rights.

Society is quickly shifting from technology known as the Internet to the broader Internet of Things (IoT).[8] "[T]he [IoT] is a concept of connecting any device (so long as it has an on/off switch) to the Internet and to other connected devices."[9] The IoT "connect[s] things and people—all of which collect and share data about the way they are used and about the environment around them."[10] This new shift in technology is a major cause of concern for private citizens because current privacy laws cannot keep pace with this ever-changing digital landscape—a landscape where it is conceivable that all of one's information will pass through the IoT, and that information will not be protected under the Fourth Amendment.

Although the legal system is trying to keep pace with the digital world, the system is reactionary and will always be behind the curve of technology. Currently, the government is taking advantage of the privacy laws to the detriment of peoples' privacy rights through its use of the third-party doctrine. That is, when an individual willingly discloses information to a third-party, such as one providing banking information to his or her financial

---

perma.cc/GVN6-WFR5] (explaining new advancements in pacemaker technology).

7. *See infra* Section I.B., which provides the cases that formed the basis for this Comment's introductory hypothetical.

8. Dalmacio V. Posadas, Jr., *The Internet of Things: Abandoning the Third-Party Doctrine and Protecting Data Encryption*, 53 GONZ. L. REV. 89, 90 (2017).

9. Jen Clark, *What Is the Internet of Things*, IBM: INTERNET OF THINGS BLOG (Nov. 17, 2016), https://www.ibm.com/blogs/internet-of-things/what-is-the-iot/ [https://perma.cc/S3RQ-CZZB].

10. *Id.*

institution, that individual loses his or her reasonable expectation of privacy in the material disclosed.[11] Thus, courts will not provide Fourth Amendment protections if the government obtains information that is in the custody of a third party.[12] To date, it is widely accepted that the third-party doctrine allows the government to access an individual's personal information stored by digital data providers because that information is considered voluntarily provided.[13] Accordingly, if current constitutional doctrines are not amended to protect citizens in the digital age, then it is conceivable that government officials will have unregulated access to an individual's personal information that is stored, monitored, and analyzed by various companies, creating an all-inclusive picture of any IoT user.

This Comment will focus on providing a solution to protect citizens' privacy in the digital age against unreasonable searches, while balancing the government's interest in obtaining evidence for criminal and civil litigation. Specifically, Part I will provide a background into the IoT and its future development in our society. Part II will discuss traditional Fourth Amendment analysis, explaining what constitutes a Fourth Amendment search, and thus, what is protected by the Constitution. Part III will discuss the history of the third-party doctrine and how its current interpretation is ill-suited for a technological society. Part IV will provide an analysis of Fourth Amendment jurisprudence in the digital age, discussing two key Supreme Court decisions that highlight the dangers of the third-party doctrine and current privacy law as it relates to technology. Part V will provide a description of the Stored Communications Act (SCA) given that the government is using this statute as a way of circumventing a citizen's Fourth Amendment protections. Part VI will discuss the Supreme Court's attempt to limit the third-party doctrine as it pertains to historical cell-site location information (CSLI) in *Carpenter v. United States*.[14] Lastly, Part VII draws from Justice Gorsuch's dissenting opinion in *Carpenter*[15] and proposes the

11. *See* Posadas, *supra* note 8, at 102.
12. *See id.*
13. *See id.*
14. 138 S. Ct. 2206 (2018).
15. *Id.* at 2261–72 (Gorsuch, J., dissenting).

creation of the "adhesion bailment" doctrine as a solution for saving the Fourth Amendment from the third-party doctrine in the digital age.

I. THE INTERNET OF THINGS

The IoT can be defined as a global platform that connects sensors to objects, providing those objects with the ability to communicate with one another via the internet.[16] For example, in Philadelphia, self-reporting trash compactors feature sensors that alert the compactor to compact the trash as it reaches a certain level, and connects to the Philadelphia Streets Department providing data on how full its compactors are, whether they need to be emptied, and whether maintenance or repair is required.[17] IoT technology provides data processing, storage, and analysis all in real-time applications.[18] Two of the largest implementations of IoT technology are found in the creation of the smart home and the smart city.

A. *The Integration of the Smart Home and City*

The smart home is not the wave of the future. It is already here, given that just about all of the technology found in one's living space has a smart home alternative.[19] A smart home is a residence that uses internet-connected devices to manage and monitor everyday living and use of one's home.[20] Devices like thermostats, televisions, locks, garage door openers, and security systems are just a few of the devices that can interconnect with a home's

16. *See* Clark, *supra* note 9.

17. Stéphane Bourgeois, *The Internet of Things in Real Life: 6 IoT Examples*, BELDEN: EMERGING TECH. & APPLICATIONS BLOG (June 9, 2017) https://www.belden.com/blog/smart-building/the-internet-of-things-in-real-life-6-iot-examples [https://perma.cc/9VCR-FQPM].

18. Posadas, *supra* note 8, at 93 (citing Leon Hounshell, *Forecasting Profitable Models for the Internet of Things*, FORBES (Mar. 23, 2017, 8:00 AM), https://www.forbes.com/sites/forbestechcouncil/2017/03/23/forecasting-profitable-models-for-the-internet-of-things/#71b98c583e94) [https://perma.cc/X5VK-PJMD].

19. Margaret Rouse, *Cutting Edge: IT's Guide to Edge Data Centers*, IOT AGENDA, https://internetofthingsagenda.techtarget.com/definition/smart-home-or-building [https://perma.cc/RZ8W-KSXC] (last visited Sept. 27, 2019).

20. *Id.*

wireless network making life more efficient.[21] Although these devices make life easier, they also store, compile, and analyze each and every moment of one's day.[22]

Just as technology companies are streamlining the home with digital technology, local governments have also begun implementing IoT technology into its cities.[23] For example, in 2018, Columbus, Ohio, implemented a connected vehicle system that alerts drivers about related driving behavior patterns in their respective driving areas, and alerts drivers to all objects surrounding the vehicle.[24] This system will eventually provide drivers, specifically first responders, with enhanced accident reports and real-time data regarding high-traffic areas—all geared toward improving citizen safety.[25]

The technological advances of society are creating a vast world that makes life easier, more manageable, and safer. However, as the IoT continues to develop, the risk of losing Fourth Amendment protections will continue to increase. For instance, the hypotheticals in this Comment's Introduction were not provided to illustrate what will eventually happen—they are situations that have already taken place, as demonstrated in the two cases below.

---

21. *See id.* For an illustration of how smart home technology provides for a more efficient life, consider the following example:

> Imagine you wake up at 7am every day to go to work. Your alarm clock does the job of waking you just fine. That is, until something goes wrong. Your train's cancelled and you have to drive to work instead. The only problem is that it takes longer to drive, and you would have needed to get up at 6:45am to avoid being late. Oh, and it's pouring with rain, so you'll need to drive slower than usual. A connected or IoT-enabled alarm clock would reset itself based on all these factors, to ensure you got to work on time. It could recognize that your usual train is cancelled, calculate the driving distance and travel time for your alternative route to work, check the weather and factor in slower travelling speed because of heavy rain, and calculate when it needs to wake you up so you're not late. If it's super-smart, [it] might even sync with your IoT-enabled coffee maker, to ensure your morning caffeine's ready to go when you get up.

Clark, *supra* note 9.

22. Posadas, *supra* note 8, at 97–98.

23. *See id.* at 97.

24. *See* Nicole George, *The Top Smart Cities*, ALLCONNECT (June 28, 2018) https://www.allconnect.com/blog/top-us-smart-cities-to-watch/ [https://perma.cc/BPN4-6L2T].

25. *Id.*

B. *Cases Illustrating a Decreased Expectation of Privacy in the Digital Age*

In 2017, Timothy Verrill was charged with murdering Christine Sullivan and Jenna Pellegrini in Ms. Sullivan's New Hampshire home.[26] New Hampshire prosecutors believed that an Amazon Echo which belonged to the victim contained evidence of the murders.[27] The judge overseeing Verrill's trial issued a court order directing Amazon to produce records created between January 27 and January 29, 2017, under a theory that the Amazon Echo may have activated and thus recorded the victims' final moments.[28]

In 2016, Ross Compton was suspected and later indicted on felony charges of aggravated arson and insurance fraud for allegedly starting a fire in his Middletown, Ohio home, based in part on evidence found on his pacemaker.[29] The government used the data found on Compton's pacemaker to prove that he was not physically capable of performing the tasks he claimed to have accomplished during the night of the fire.[30] Police obtained a search warrant for data recorded on the pacemaker and, after medical technicians downloaded the data revealing heart rate and cardiac rhythms before, during, and after the fire, the police subpoenaed and ultimately obtained the data.[31]

---

26. Kimberly Haas, *Murder Victims' Families Upset They Weren't Warned About Recordings*, N.H. UNION LEADER (Nov. 14, 2018) https://www.unionleader.com/news/courts/murder-victims-families-upset-they-weren-t-warned-about-recordings/article_c75ceeec-69a2-54d8-b20f-2ad5f6fecf9c.html [https://perma.cc/HBJ6-RMG2].

27. *Id.*

28. *Id.*

29. Lauren Pack, *Arson Suspect in Unique Case Featuring Pacemaker Data is Back in Custody*, JOURNAL-NEWS (July 24, 2018) https://www.journal-news.com/news/arson-suspect-unique-case-featuring-pacemaker-data-back-custody/dn6JyzsOemZovpayJMZLNJ/ [https://perma.cc/DRK5-SAGG].

30. *See id.* Mr. Compton claimed that when he awoke from the fire, he packed his belongings in multiple bags, grabbed his computer and medical device charger, broke a window with his cane, and threw his luggage out of it before abandoning his home. Deanna Paul, *Your Own Pacemaker Can Now Testify Against You in Court*, WIRED (July 29, 2017, 7:00 AM), https://www.wired.com/story/your-own-pacemaker-can-now-testify-against-you-in-court/ [https://perma.cc/TP7R-JG8Q].

31. Paul, *supra* note 30.

The cases presented above illustrate how stored data that is transmitted through digitally connected devices provide the government a way of accessing personal information without the need for a warrant. The government is simply obtaining a subpoena or court order for the data that was transmitted and now stored with a third-party. The development of stronger connectivity, intelligence, and convenience functions on digital devices creates a greater risk of private data being exposed to the outside world.[32] Stephanie Lacambra, the Electronic Frontier Foundation's criminal defense attorney, sums up Compton's case, and the disturbing truth of the digital world:

> The reality is that we are no longer the sole proprietors or controllers of our personal information . . . . For people worried about being monitored in that way, this ruling is chilling. If Compton didn't want doctors and law enforcement to have access to his heartbeat, what alternative did he have—decide against getting a pacemaker?[33]

Using the newest innovative technological gadgets leaves citizens and their property vulnerable to third-party technology providers. With the implementation of smart homes and cities, citizens will have no choice but to share their information with third parties, forcing private citizens to integrate into the IoT. Accordingly, the duty to protect an individual's privacy is incumbent upon citizens, legislators, and the courts to ensure that the Fourth Amendment remains intact and continues to protect the nation's citizens from unlawful searches. To accomplish this goal, legislatures must modify current laws so the government cannot compel technology companies to provide access to stored data,[34] and courts should reevaluate the third-party doctrine in the digital age.[35] One must first understand the history of Fourth Amendment jurisprudence, as described in the next section, in order to see the extent of the concerns raised by the IoT and the

32. *See id.*
33. *Id.* (internal quotation marks omitted).
34. *See infra* Part V.
35. *See infra* Part III.

third-party doctrine and appreciate the need for enhanced privacy rights in a technological society.

II. TRADITIONAL FOURTH AMENDMENT ANALYSIS

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[36] As illustrated in *United States v. Jones*, there are currently two approaches courts use to analyze whether the government conducted a Fourth Amendment search.[37] The first approach, developed in *Olmstead v. United States*, is known as the physical trespass test.[38] If the government physically trespasses on an individual's constitutionally protected property for the purpose of obtaining information, courts will generally conclude that a Fourth Amendment search occurred.[39] Under the second approach, outlined in Justice Harlan's concurrence in *Katz v. United States*, courts will likely conclude that a Fourth Amendment search took place if the government violates an individual's reasonable expectation of privacy.[40] The *Katz* test has two requirements: first, the individual must display a subjective expectation of privacy, and second, that expectation must be one that society is willing to recognize as reasonable.[41]

Originally, the Court in *Katz* appeared to replace the physical trespass test created in *Olmstead v. United States*.[42] The *Jones* Court made it clear, however, that Justice Harlan's reasonable expectation of privacy analysis in *Katz* did not extinguish the "physical trespass" rule: "The *Katz* reasonable-expectations test 'has been *added* to, not *substituted* for,' the traditional property-based understanding of the Fourth Amendment . . . ."[43] Although courts still utilize the physical trespass test, Fourth Amendment

36. U.S. CONST. amend. IV.

37. *See* United States v. Jones, 565 U.S. 400, 411 (2012).

38. *See* Olmstead v. United States, 277 U.S. 438, 464–66 (1928).

39. *See id.* (holding that wiretapping did not amount to search within meaning of Fourth Amendment because there was no actual physical invasion of defendant's house or curtilage for purpose of making seizure).

40. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

41. *Id.*

42. *Id*. at 353 (majority opinion).

43. Florida v. Jardines, 569 U.S. 1, 11 (2013) (quoting United States v. Jones, 565 U.S. 400, 409 (1928)).

search analysis is generally conducted using the far murkier reasonable expectation of privacy test created in *Katz*.[44]

Accordingly, an individual may be entitled to Fourth Amendment protection of "what he seeks to preserve as private, even in an area accessible to the public."[45] Therefore, Fourth Amendment protection does not necessarily depend on the material sought, but rather on the relationship the individual creates with the information and his surroundings that give rise to an expectation of privacy.[46] This premise was first illustrated in *Katz*:

> The Government stresses the fact that the telephone booth from which the petitioner made his calls was constructed partly of glass, so that he was as visible after he entered it as he would have been if he had remained outside. But what he sought to exclude when he entered the booth was not the intruding eye—it was the uninvited ear. He did not shed his right to do so simply because he made his calls from a place where he might be seen.[47]

Thus, the question that must be answered is: How can the judiciary continue to provide privacy protection to citizens in the digital age? Interestingly enough, the *Jones* Court's analysis suggests that the presence of technological devices may diminish an individual's reasonable expectation of privacy for purposes of defining a Fourth Amendment search.[48] In its analysis, the Court reintroduced the old physical trespass test under the Fourth Amendment to ensure strong protections for individual privacy.[49] Before discussing the Court's blended analysis under *Jones*, this

---

44. *See Katz*, 389 U.S. at 360–61 (Harlan, J., concurring) (likening electronic intrusion to physical intrusion).

45. *Id*. at 351–52 (majority opinion).

46. *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 822 (2004) ("The 'critical' fact was the relationship that Katz had established when he occupied the phone booth, shut the door behind him, and 'pa[id] the toll that permit[ted] him to place a call.'" (quoting *Katz*, 389 U.S. at 361 (Harlan, J., concurring))).

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

48. *Jones*, 565 U.S. at 404–05 (holding government installation of GPS device and subsequent analysis of data constitutes Fourth Amendment search because government physically occupied private property to obtain information).

49. *See* discussion of *Jones*, *infra* Section IV.B.

Comment will first provide a background of the third-party doctrine and highlight the dangers of losing all Fourth Amendment protection if the third-party doctrine is not interpreted in a way that suits the digital age.

III. THE THIRD-PARTY DOCTRINE

An individual generally does not have a reasonable expectation of privacy when he or she voluntarily discloses information to a third party.[50] As it stands, the current interpretation of the third-party doctrine took shape after the Court's rulings in two cases, *United States v. Miller*[51] and *Smith v. Maryland*.[52] In *Miller*, the government subpoenaed two banks where the defendant had accounts.[53] The subpoenas required the banks to produce all of the defendant's accounts, which the Court described as "negotiable instruments to be used in commercial transactions."[54] The defendant sought to suppress the bank records, arguing that the government conducted an unreasonable search in violation of the Fourth Amendment.[55] The Court disagreed with the defendant's argument and found that:

> The [bank] 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.[56]

Three years later, in *Smith v. Maryland*, the Court addressed whether the government's use of a pen register violated the

---

50. Posadas, *supra* note 8, at 102; s*ee also* United States v. White, 401 U.S. 745, 751, 753 (1971) (holding government's use of agents who themselves may reveal contents of conversations with an accused does not violate Fourth Amendment).

51. United States v. Miller, 425 U.S. 435 (1976).

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

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

54. *Id.* at 437–38, 442.

55. *See id.* at 438, 442.

56. *Id.* at 443 (citations omitted).

defendant's Fourth Amendment rights.[57] "A pen register is a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released. It does not overhear oral communications and does not indicate whether calls are actually completed."[58] The Court found, as it did in *Miller*, that the defendant voluntarily conveyed the subject information (the numbers he dialed) to a third party (the telephone company) when he placed his calls through an operator.[59] The Court recognized that the phone company recorded the numerical information at issue "for a variety of legitimate business purposes."[60] Thus, when the defendant used his phone, "he assumed the risk that the [phone] company would reveal to police the numbers he dialed."[61]

In today's technological world, scholars question whether the current interpretation of the third-party doctrine should be strictly applied.[62] The doctrine creates a diminished expectation of privacy in information that one voluntarily shares.[63] However, as the IoT continues to advance, the expectation of privacy established under the third-party doctrine constantly diminishes as a result of individuals losing the choice of whether to share information because their lives are constantly streaming through the IoT for commercial purposes. Moreover, the way the government is using the third-party doctrine bypasses the physical trespass form of a search, given that no agent or officer has to physically intrude on an individual's property; the government can simply obtain a court order or subpoena and compel the company to release the stored information the government seeks,[64] essentially robbing individuals of their privacy rights.

---

57. *Smith*, 442 U.S. at 736.

58. *Id.* at 736 n.1 (quoting United States v. N.Y. Tel. Co., 434 U.S. 159, 161 n.1 (1977)).

59. *Id.* at 743–44.

60. *Id.* at 743.

61. *Id.* at 744.

62. Lucas Issacharoff & Kyle Wirshba, *Restoring Reason to the Third Party Doctrine*, 100 MINN. L. REV. 985, 987–988 (2016).

63. *See Smith*, 442 U.S. at 743–44.

64. *See* 18 U.S.C. § 2703 (2012); *see also* Pfeifle, *supra* note 4 at 431 ("[I]nformation obtained from storage receives a more relaxed standard than information obtained in transit.").

Thus, in light of technological globalization, one now assumes the risk that when he or she uses devices that transmit data to third-party companies, the information is automatically disentitled to Fourth Amendment protection. Because technology is rapidly advancing, more guidance is needed to determine when the Fourth Amendment should apply. Further, the third-party doctrine needs to be clearly defined to provide citizens with an understanding of what constitutes a reasonable expectation of privacy in data shared and stored on the IoT. Hence, Part IV will discuss the Supreme Court's attempt to provide some level of defense against losing Fourth Amendment protection in the digital age, and Part V will discuss statutory protection and illustrate how some forward-thinking States are implementing law that will not allow the government to continue to rely on *Smith*, *Miller*, and the third-party doctrine in the technological era.

IV. FOURTH AMENDMENT ANALYSIS IN THE DIGITAL AGE

As technology has evolved, so has the Court's interpretation of the Fourth Amendment, albeit slowly. The two cases discussed below not only highlight the Court's analysis of the Fourth Amendment and how it interacts with technology, but also provide a warning that privacy laws must be amended to suit the digital age.[65] The Court must acclimatize its understanding and modify Fourth Amendment jurisprudence to suit the evolution of technology, because as it currently stands, most citizens do not feel they have any expectation of privacy in the digital age.[66]

A. *Thermal Imaging* – Kyllo v. United States

In *Kyllo*, government agents used a thermal imaging device to inspect the interior of the defendant's home from a public street to gather evidence on the possibility that the defendant was growing marijuana.[67] The thermal imaging device used by the government "detect[s] infrared radiation, which virtually all objects emit but

65. *See* United States v. Jones, 565 U.S. 400 (2012); Kyllo v. United States, 533 U.S. 27 (2001).

66. *See* Cameron F. Kerry, *Why Protecting Privacy is a Losing Game Today—And How to Change the Game*, BROOKINGS (July 12, 2018) https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/ [https://perma.cc/ZN3A-THSB].

67. *Kyllo*, 533 U.S. at 29–30.

which is not visible by the naked eye . . . [and] converts [that] radiation into images based on relative warmth . . . operat[ing] somewhat like a video camera showing heat images."[68] The scan revealed that some portions of Kyllo's home were warmer than others, and significantly warmer than his neighbors' homes.[69] The Court held that when the government, even from a public viewpoint, "obtain[s] by sense-enhancing technology any information regarding the interior of the home that could not otherwise be obtained without physical 'intrusion into a constitutionally protected area' . . . a search [has occurred]—at least where (as here) the technology in question is not in general public use."[70]

The aspect of *Kyllo* most relevant to this discussion is that the Court found that technology has decreased the level of protection the Fourth Amendment provides.[71] However, the Court concluded by clearly stating that there is a high level of protection when dealing with searches of a person's home: "We have said that the Fourth Amendment draws 'a firm line at the entrance to the house,' [and] [t]hat line, we think, must be not only firm but also bright—which requires clear specification of those methods of surveillance that require a warrant."[72] Hence, the government's activity being deemed a Fourth Amendment search was not contingent on the *level* of intimacy of the information actually collected through sense-enhancing technology, but rather that *all* details of the home are considered intimate for the purposes of the Fourth Amendment.[73] The Court undoubtedly provides a high level of protection to all activities that take place in the home.

---

68. *Id.* at 30–31.

69. *Id.* at 30.

70. *Id.* at 34 (citations omitted) (quoting Silverman v. United States, 365 U.S. 505, 512 (1961)).

71. *See id.* at 33–34.

72. *Id.* at 40 (citation omitted) (quoting Payton v. New York, 445 U.S. 573, 590 (1980)).

73. *See id.* at 37–38. The government argued that the Court could develop a rule that would limit the prohibition of thermal imaging to "intimate details"; however, the Court found that argument not only wrong in principle but impractical. *Id.* at 38. The use of thermal vision would allow the government to see not only any illegal activity but all activities; for example, the Court noted that the use of thermal imaging could detect when the "lady of the house" takes a bath—a detail that many would consider intimate. *Id.*

However, even though *Kyllo* clearly provides a high level of Fourth Amendment protection in the home, the Court has not provided a solution for citizens to continue enjoying the same level of privacy in the wake of the digital age. *Kyllo*'s holding leaves open the possibility that one's privacy rights will shrink as technology advances given that a substantial amount of what the government utilizes to gather information is available to the general public. For example, thermal imaging devices are now at the fingertips of most citizens; the government can accordingly argue that they no longer intrude on an individual's constitutionally protected right because of the public's newfound access to thermal-imaging technology.[74] Thus, in order to maintain Fourth Amendment protection in the digital age, the Court must overturn in part *Kyllo*'s holding.

B. *GPS Tracking Devices* – United States v. Jones

In *Jones*, the government placed Antoine Jones, a nightclub owner and operator, under investigation for the alleged trafficking of narcotics.[75] Based on the government's investigation, the FBI applied for a warrant authorizing the placement of a Global Positioning System (GPS) tracking device on Jones's automobile.[76] Once obtained, the FBI placed the GPS tracking device on the undercarriage of Jones's vehicle and monitored its movement twenty-four hours a day for approximately twenty-eight days.[77] During the period Jones's vehicle was monitored, the FBI collected more than 2,000 pages of data detailing the vehicle's location.[78]

However, the warrant as implemented was invalid,[79] so the Court had to considered whether the government's actions amounted to a Fourth Amendment search and thus whether a

74. *See* FLIR ONE Gen 3, FLIR, https://www.flir.com/products/flir-one-gen-3/?model=435-0005-02&pi_ad_id=%7Bcreative%7D&creative=11174160 4345&keyword=&matchtype=&network=g&device=c&gclid=EAIaIQobChMIu embk8LS4AIVB4TICh1NpAGvEAQYASABEgIDDvD_BwE [https://perma.cc/ FS78-WUMF] (last visited on Oct. 25, 2019).

75. United States v. Jones, 565 U.S. 400, 402 (2012).

76. *Id.*

77. *Id.* at 402–03.

78. *Id.* at 403.

79. *See id.* at 402–403. ("A warrant [was] issued, authorizing installation of the [GPS] device in the District of Columbia . . . within 10 days. On the 11th day, and not in the District of Columbia but in Maryland, agents installed a GPS tracking device on the undercarriage of the Jeep . . . .").

warrant was even required.[80] The Court held that the attachment of a GPS device to a vehicle, "and subsequent use of that device to monitor the vehicle's movements," constituted a search under the Fourth Amendment.[81] Interestingly, Justice Scalia focused his analysis on the government's physical trespass, rather than Jones's reasonable expectation of privacy.[82] The majority did not disturb the reasonable expectation of privacy test defined in *Katz*.[83]

Prior to *Jones*, Fourth Amendment analysis of the same issue would have focused solely on whether the individual had a reasonable expectation of privacy, which could have led to a different outcome.[84] *Jones* instead provided the courts with an alternative means of establishing a Fourth Amendment search; that is, by showing a governmental intrusion of a protected property interest.[85] Given that the reasonable expectation of privacy analysis relies in part on objective means—an expectation of privacy that society is willing to accept as reasonable—it seems that Justice Scalia recognized that the prevalence of technological devices would in fact diminish objective expectations of privacy and thus reintroduced the property-based approach to Fourth Amendment search analysis.

The concurring Justices in *Jones* agreed that there was a Fourth Amendment search, but on different grounds.[86] Justice Sotomayor's concurrence is particularly notable because she explicitly stated that the time has come to revisit and alter the third-party doctrine as it applies in the digital age:

> 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

80. *See id.* at 404–05.

81. *Id.* at 402.

82. *See id.* at 411.

83. *Id.*

84. *See* United States v. Knotts, 460 U.S. 276, 281 (1983) ("A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy.").

85. *See Jones*, 565 U.S. at 406–07.

86. *Id.* at 413, 415 (Sotomayor, J., concurring) (accepting the majority's property-based approach but also arguing that the long-term use of the GPS would indeed violate the defendant's reasonable expectation of privacy); *id.* at 419 (Alito, J., concurring) (agreeing a Fourth Amendment search occurred, but arguing that the Court should have analyzed the case using the *Katz* test).

> 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. . . . I for one doubt that people would accept without complaint the warrantless disclosure to the government of a list of every Web site they had visited in the last week, or month, or year.[87]

Justice Sotomayor argued that Fourth Amendment jurisprudence should stop treating secrecy as a requirement for privacy.[88] "[One] would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection."[89] Justice Sotomayor contended that the third-party doctrine, as it stands now, is unsuitable for a digital world.[90] Her position becomes more relevant as the IoT continues to grow—as more devices monitor one's activities, an individual's reasonable expectation of privacy will eventually cease to exist.

V. FEDERAL PRIVACY LAWS FAIL IN THE IOT

As Fourth Amendment jurisprudence evolved, Congress realized that advancing technology could lead to potential inconsistencies in applying this developing area of law.[91] Congress's concern of advancing technology prompted it to commission its Office of Technology Assessment (OTA) to provide guidance regarding how the Fourth Amendment should apply as technology progressed.[92] In 1985, the OTA generated a report

87. *Id.* at 417–18 (Sotomayor, J., concurring) (citations omitted).

88. *Id.* at 418.

89. *Id.* (citing Smith v. Maryland, 442 U.S. 735, 742 (1979) (Marshall, J., dissenting) and Katz v. United States, 389 U.S. 347, 351–52 (1967)).

90. *Id.* at 417.

91. Allegra Bianchini, Note, *Always On, Always Listening: Navigating Fourth Amendment Rights in a Smart Home*, 86 GEO. WASH. L. REV. ARGUENDO 1, 16 (2018).

92. *Id.*

concluding that privacy protection was "weak, ambiguous, or nonexistent," despite Supreme Court guidance.[93] Based on the findings of the OTA's report, Congress enacted the Electronic Communications Privacy Act (ECPA) to address the lack of Fourth Amendment protection caused by the third-party doctrine.[94]

As a subsection of the ECPA, Congress enacted the Stored Communications Act (SCA), which was premised on the theory that the proprietary interest of information should not change based solely upon a third-party service provider electronically storing that information rather than the owner.[95] Electronic storage means "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof;" and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication."[96] As this Comment will illustrate below, the SCA's protections are inadequate in the face of a modern technological world.[97]

A. *Rules of Compelled Disclosure by the Government*

The SCA was promulgated to maintain an individual's reasonable expectation of privacy even where communications are stored with a service provider despite the third-party doctrine.[98] However, one component of the SCA, "compelled disclosure," allows the government to obtain data stored with a service provider without a warrant in certain situations.[99] Whether the government needs a warrant, or a mere court order or subpoena, depends on the level of protection the stored information is afforded.[100] The SCA determines the level of protection afforded to stored information by

93. *Id.* (quoting OFFICE OF TECH. ASSESSMENT, U.S. CONG., OTA-CIT-293, FEDERAL GOVERNMENT INFORMATION TECHNOLOGY: ELECTRONIC SURVEILLANCE AND CIVIL LIBERTIES 45 (1985)).

94. *Id* at 17.

95. *Id.*

96. 18 U.S.C. § 2510(17) (2012).

97. Bianchini, *supra* note 91, at 17–18.

98. Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 816 (2003).

99. 18 U.S.C. § 2703 (2012); *see also* Kerr, *supra* note 98, at 816.

100. *See* § 2703 (a)–(b).

classifying it based on three distinct categories: the type of service provided, the type of information sought, and the length of time for which the information is stored.[101]

1. Electronic Communications Service v. Remote Computing Service

Under the SCA, a provider can either be an Electronic Communications Service (ECS), which provides its users "the ability to send or receive wire or electronic communications" or a Remote Computing Service (RCS), which provides its users online "storage or processing services."[102] Determining the service provider's designation is not based on the provider's status in the abstract, but rather the provider's interaction with a particular communication; a given provider can be classified as an ECS at one point and an RCS at another.[103] For example, when someone sends an electronic communication to another, the provider is an ECS until the message is opened.[104] If the recipient of the information decides to save the message for future reference, then the same provider is now acting as an RCS in storing that communication.[105] A court's classification is important because an ECS provider is afforded more protection than an RCS provider.[106]

2. Content v. Non–Content

The second category is based upon what type of information the government wants to obtain—content or non-content.[107] "Content" is the information in the communication that one intends to share

101. § 2703; Bianchini, *supra* note 91, at 18; *see also* 18 U.S.C. § 2702 (2012) (providing rules that govern when an Internet Service Provider (ISP) can voluntarily disclose information to the government).

102. *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1214 (2004) (quoting 18 U.S.C. §§ 2510(15), 2711(2)).

103. Eric R. Hinz, *A Distinctionless Distinction: Why the RCS/ECS Distinction in the Stored Communications Act Does Not Work*, 88 NOTRE DAME L. REV. 489, 496 (2012).

104. *Id.*

105. *Id.*

106. *See id.* at 500–01 (illustrating the fact that RCS is afforded a lower threshold of protection).

107. *See* Bianchini, *supra* note 91, at 18.

with another.[108] The body of the message in an email would be considered the "content."[109] In contrast, "non-content," also referred to as metadata, is what the provider uses to deliver and process the communication.[110] For example, the name and email address of the recipient would be considered "non-content" information.[111] The SCA provides greater protection to "content" information because messages intended for a certain recipient implicate greater privacy concerns.[112]

3. Time in Storage

The third category is based on the amount of time that a communication is stored.[113] Communications stored for 180 or fewer days and those stored longer than 180 days are provided different levels of protection.[114] For example, if a communication that is considered "content" (unopened email)[115] is held within an ECS for 100 days, the government must obtain a warrant pursuant to section 2703(a) of the SCA to access that data.[116] However, if that same communication is stored longer than 180 days, then the government need only obtain a court order or subpoena pursuant to section 2703(d).[117]

B. *Rules of Compelled Disclosure Fail in an IoT World*

A court's characterization of information under the SCA will dictate how the government can compel disclosure of that information.[118] The only time the government must obtain a warrant is when an ECS provider stores "content" information that

108. Kerr, *supra* note 102, at 1228.
109. Bianchini, *supra* note 91, at 18.
110. Kerr, *supra* note 102, at 1228.
111. Bianchini, *supra* note 91, at 18.
112. *See* Kerr, *supra* note 102, at 1228.
113. *See* Christina Raquel, *Blue Skies Ahead: Clearing the Air for Information Privacy in the Cloud*, 55 SANTA CLARA L. REV. 467, 485 (2015).
114. *See id.*
115. *See* Kerr, *supra* note 102, at 1216 ("[W]hen an e-mail customer leaves a copy of an already-accessed e-mail stored on a server, that copy is no longer 'incident to transmission' . . . rather, it is just in remote storage like any other file held by an RCS.").
116. 18 U.S.C. § 2703(a) (2012).
117. *Id.*
118. *See* Bianchini, *supra* note 91, at 18.

is held for fewer than 180 days; in all other instances, the government need only obtain a subpoena or court order to obtain the sought-after information.[119] If that fact is not chilling enough, technology has advanced to a point where these simple rules, which appear to favor the government, have become blurred.

In today's technological society, service providers can perform the functions of an ECS and RCS simultaneously,[120] and distinctions between "content" and "non-content" information have become unclear.[121] For example, if providers can perform ECS and RCS functions simultaneously, then the government can classify the provider as an RCS and simply obtain a court order pursuant to section 2703(d), or provide the customer notice and subpoena the information; the government can delay notice up to ninety days, however, if notification would have adverse results.[122] Moreover, the government may forego attempting to obtain "content" information given that "non-content" data can now reveal intimate details about our lives; according to NSA's former general counsel, Stewart Baker, "[m]etadata absolutely tells you everything about somebody's life."[123]

As a result, the SCA fails to provide the level of protection needed from government intrusion, especially in an IoT world where a third-party provider will constantly stream and store one's private information. Although new statutes and case law are recognizing the need for more privacy protection in the digital age, the legislature and judiciary are failing to keep up with advancements in technology.[124]

---

119. *See* Hinz, *supra* note 103, at 501. The standard for a court order is much lower than the probable cause standard needed for a warrant. *See* § 2703(d) ("A court order for disclosure . . . shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication . . . are relevant and material to an ongoing criminal investigation.").

120. Bianchini, *supra* note 91, at 18.

121. *See id.* at 19; Kerr, *supra* note 102, at 1227–28 (discussing the difficulties in distinguishing "content" from "non-content" information).

122. *See* Hinz, *supra* note 103, at 501; *see also* 18 U.S.C. § 2705(a)(2) (2012) (providing the ways in which the government may delay notice because of an "adverse result").

123. LAURA K. DONOHUE, THE FUTURE OF FOREIGN INTELLIGENCE*:* PRIVACY AND SURVEILLANCE IN A DIGITAL AGE 39 (2016).

124. *See* California Electronic Communications Privacy Act, CAL. PENAL CODE § 1546.1 (West 2017). This statute mandates that the government obtain

VI. PIERCING THE ARMOR OF THE THIRD-PARTY DOCTRINE – THE SUPREME COURT'S DECISION IN *UNITED STATES V. CARPENTER*

In *Riley v. California*, the Court held that a warrantless search of a cell phone was not reasonable, even where the cell phone was seized from the defendant's body incident to arrest.[125] The Court reasoned that a cell phone required heightened protection given the amount of data that can be stored on each device; that is, cell phones can contain essentially every facet of an individual's life.[126] The *Riley* decision was appealing because the Court appeared to signal its recognition that Fourth Amendment jurisprudence needed adjusting to accommodate a digital world. There is a significant amount of language in the Court's decision that suggests *Riley* is just "the tip of the iceberg" because "[w]e're now in a 'digital age' and quantity of data and the 'qualitatively different' nature of at least some digital records changes how the Fourth Amendment

a warrant and particularly describe the electronic communication the government intends to search, and requires the government to provide notice to the target of the warrant. *Id.* Furthermore, the statute provides protection to many more companies given the statute's broad definition of "service provider." *Id.* § 1546(j). However, when information is sent without human involvement (as it does with the Amazon Edge), when and how information becomes an electronic communication is unclear. Because the definition of a "service provider" is dependent on whether it provides the user the ability to send or receive electronic communications, the government can still argue its away around the warrant requirement. *Id.*; Pfeifle, *supra* note 4 at 434–37. For other examples of attempts to provide consumers with greater protection, see, *e.g.*, MONT. CODE ANN. §§ 46-5-601 to -605 (West 2017) (requiring the government to obtain a warrant prior to compelling a provider to disclose a user's communication, but still allowing the government to prevent providers from notifying its customers of the disclosure); United States v. Warshak, 631 F.3d 266, 284, 286–87 (6th Cir. 2010) (holding that a user has a reasonable expectation of privacy in their email, and concluding that even where a user agrees to provide the user's internet service provider (ISP) with access to their emails, that is not enough to defeat Fourth Amendment protections).

125. Riley v. California, 573 U.S. 373, 386 (2014).

126. *Id.* at 393 ("The term 'cell phone' is itself misleading . . . many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. . . . One of the most notable distinguishing features of modern cell phones is their immense storage capacity.").

should apply."[127] Nevertheless, the Court limited its ruling to cases that involve a search incident to arrest.[128]

The Court answered the question regarding aggregated digital information in *United States v. Carpenter*.[129] The majority opinion, authored by Chief Justice Roberts—who also authored *Riley*—held that a cell phone user has a reasonable expectation of privacy in his cell phone's geolocation data.[130] The Court focused on guideposts created by prior case law, specifically how the Fourth Amendment seeks to secure "'the privacies of life' against 'arbitrary power'"[131] and "to place obstacles in the way of a too permeating police surveillance."[132]

Prior to *Carpenter*, the government could compel cell phone carriers under the SCA to turn over a user's cell-site location information (CSLI) whenever it could offer "'specific and articulable facts showing that there are reasonable grounds to believe' that the records sought 'are relevant and material to an ongoing criminal investigation.'"[133] CSLI is generated from cell phones sending signals to and from "cell sites," which are radio antennas mounted on "tower[s] . . . light posts, flag poles, church steeples, or the sides of buildings."[134] Whenever a cell phone user sends or receives a text, phone call, or uses data, that individual creates CSLI.[135] Most notably, the SCA's requirement for the government to obtain a user's CSLI is a lower standard than the probable cause standard required for warrants.

In 2011, the police arrested four men suspected in a string of robberies in Detroit, Michigan.[136] One of the men confessed to all of the robberies and provided officers with his call records from the

127. Orin S. Kerr, *The Significance of* Riley, WASH. POST: VOLOKH CONSPIRACY (June 25, 2014), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/06/25/the-significance-of riley/ [https://perma.cc/5FLN-7RRT].

128. *Riley*, 573 U.S. at 395 n.1.

129. United States v. Carpenter, 138 S. Ct. 2206, 2211 (2018).

130. *Id.* at 2219.

131. *Id.* at 2214 (quoting Boyd v. United States 116 U.S. 616, 630 (1986)).

132. *Id.* (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)).

133. *Id.* at 2212 (quoting 18 U.S.C. § 2703(d)).

134. *Id.* at 2211.

135. *Id.*

136. *Id.* at 2212.

time of the robberies, a list of suspects, and their phone numbers.[137] Armed with that information, "the prosecutors applied for court orders under the Stored Communications Act to obtain cell phone records for petitioner Timothy Carpenter and several other suspects."[138] Federal magistrate judges granted the prosecutors' requests and ordered MetroPCS and Sprint, two wireless carriers with whom Carpenter had accounts, to disclose CSLI for the "origination and . . . termination [of] incoming and outgoing calls" to Carpenter's cell phone during the period in which the robberies occurred.[139] As a result, "the Government obtained 12,898 location points cataloging Carpenter's movements—an average of 101 data points per day."[140] With that information, the government was able to show that Carpenter was present at several of the crimes scenes at the times during which the robberies occurred.[141] After presenting this information at trial, Carpenter was convicted on all but one count and received a sentence of more than 100 years in prison.[142]

Following his conviction, Carpenter appealed to the Sixth Circuit.[143] The Sixth Circuit affirmed the lower court and held that "Carpenter lacked a reasonable expectation of privacy in the location information collected by the FBI because he shared that information with his wireless carriers."[144] The Sixth Circuit concluded that because "cell phone users voluntarily convey cell-site data to their carriers as 'a means of establishing communication,'" the CSLI is not entitled to Fourth Amendment protection.[145] Carpenter then filed for a petition of certiorari, which the Supreme Court granted.[146]

---

137. *Id.*
138. *Id.*
139. *Id.*
140. *Id.*
141. *Id.* at 2212–13.
142. *Id*. at 2213.
143. *See id.*
144. *Id.*
145. *Id.* (quoting United States v. Carpenter, 819 F.3d 880, 888 (6th Cir. 2016)).
146. *Id.*

Carpenter is a unique case given that the majority recognized something "qualitatively different" in the digital data at issue.[147] Chief Justice Roberts created a unique exception because he saw government acquisition of CSLI as sitting "at the intersection of two lines of cases, both of which inform our understanding of the privacy interest at stake."[148] The first line of cases "addresses a person's expectation of privacy in his physical location and movements."[149] The second set of cases relies on the third-party doctrine of *Smith* and *Miller* where Chief Justice Roberts wrote, "the Court has drawn a line between what a person keeps to himself and what he shares with others . . . [maintaining] that 'a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.'"[150] However, unlike precedent illustrating the Court's concern over technology diminishing one's reasonable expectation of privacy, Chief Justice Roberts—instead of reevaluating Fourth Amendment jurisprudence—took a novel approach and applied both lines of precedent to CSLI, balancing one's reasonable expectation of privacy in his movements against one providing his movements to a third-party.

Chief Justice Roberts found that the government invaded Carpenter's reasonable expectation of privacy in his physical movements when it accessed CSLI from Carpenter's wireless carrier.[151] In the Court's opinion, Chief Justice Roberts accounted for the advancement in a wireless carrier's capability to pinpoint an individual's location, the private nature of a person's movements and the sensitive information it may reveal, and the ability of the government "to retrace a person's whereabouts" which was subject only to a wireless carrier's five-year retention policy.[152] Chief Justice Roberts then weighed his findings against the third-party doctrine concerns of *Smith* and *Miller*.[153] He found that when looking at "the nature of the particular documents sought" to

147. *Id.* at 2216–17.

148. *Id.* at 2214–15.

149. *Id.* at 2215. Chief Justice Roberts cited to *United States v. Knotts*, 460 U.S. 276 (1983) and *United States v. Jones*, 565 U.S. 400 (2012) for the stated proposition. *Id.*

150. *Id.* at 2216 (quoting Smith v. Maryland, 442 U.S. 735, 743-44 (1979)).

151. *Id.* at 2219.

152. *Id.* at 2218.

153. *See id.* at 2219–20.

determine whether "there is a legitimate 'expectation of privacy' concerning their contents . . . the Government fail[ed] to appreciate that there [were] no comparable limitations on the revealing nature of CSLI."[154] CSLI, which is "a detailed chronicle of a person's physical presence compiled every day, every moment, over several years . . . implicates privacy concerns far beyond those considered in *Smith* and *Miller*."[155]

Chief Justice Roberts correctly recognized that the *voluntary* disclosure rationale of the third party doctrine does not make sense in the CSLI context.[156] CSLI "is not truly 'shared' as one normally understands the term," since the "sharing" occurs automatically "without any affirmative act on the part of the user beyond powering up [his cell phone]."[157] More importantly, *Carpenter* illustrated the fact that there are many digital applications from which the government could obtain copious amounts of data about an individual.[158] Instead of finding that the third-party doctrine should not apply in a digital world given that "people often *do* reasonably expect that information they entrust to third parties . . . will be kept private,"[159] the majority created a balancing test where courts must assign value to different categories of information and weigh the individual's privacy rights in that information against a third-party disclosure. Thus, the Court dispelled the notion that a person never has an expectation of privacy in digital information held by third parties.[160]

VII. THE ANSWER TO FOURTH AMENDMENT JURISPRUDENCE IN THE DIGITAL AGE – THE "ADHESION BAILMENT DOCTRINE"

As Chief Justice Roberts noted in *Carpenter*, Fourth Amendment jurisprudence is at a crossroad regarding the third-

154. *Id.* at 2219 (quoting United States v. Miller, 425 U.S. 435, 442 (1976)).
155. *Id.* at 2220.
156. *Id.*
157. *Id.*
158. *See id.* at 2262 (Gorsuch, J., dissenting).
159. *Id.* at 2263.
160. *See id.* at 2263, 2267. "[I]f the third party doctrine is supposed to represent a normative assessment of when a person should expect privacy [in information conveyed to third parties], the notion that the answer might be 'never' seems a pretty unattractive societal prescription." *Id.* at 2263.

party doctrine and advanced digital technology.[161] In an IoT world, a user's profile is created simply from that user completing everyday mundane tasks.[162] Thus, courts are left to determine whether the user-generated profiles are voluntarily conveyed, whether the information is of a type that deserves Fourth Amendment protection, and how strong the government's interests are in obtaining the user's information—a daunting task. Aside from some innovative state legislation and a novel approach that would provide an IoT user with enhanced privacy protection within their home, society remains in limbo as its reasonable expectation of privacy continues to diminish in the digital age.[163] This Comment attempts to provide a more comprehensive solution, drawing from Justice Gorsuch's dissenting opinion in *Carpenter*.

Justice Gorsuch proposed a pre-*Katz* approach that deals with problems of modern technology. The basis of his idea was simple and drew from the language of the Fourth Amendment: "[T]he traditional approach asked if a house, paper or effect was *yours* under law. No more was needed to trigger the Fourth Amendment."[164] There are several advantages of using that kind of property-based approach. Judges will have a much easier time navigating the issues of the third-party doctrine as that approach would remove from the judge "their own personal policy preferences" about the reasonableness of one's expectation of privacy and allow for "legislative participation in the Fourth

161. *See id.* at 2215–16.

162. *See supra* Part I.

163. *Supra* text accompanying note 122; *see* Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CALIF. L. REV. 805, 866–87 (2016) (providing the theory of "Digital Curtilage"). Digital Curtilage is a concept that is applied much like the traditional protection one receives from the physical curtilage that surrounds a home. *Id.* Essentially, digital curtilage would include IoT devices that are connected in the home and that communicate information that flows from the home to third-party providers. *Id.* Thus, once an IoT device is connected to a home network, the third-party doctrine should apply given the all-inclusive and intimate nature of the information contained within. *Id.* Although this approach would provide sufficient protection in an IoT user's home, the issue is that IoT devices compile data on users even when the user is traveling outside the home, such as shopping at the mall, parking a car, or ordering food. Thus, a stronger, more holistic approach is needed to provide an IoT user with adequate protection regardless of whether the individual is in the home.

164. *Carpenter*, 138 S. Ct. at 2267–68.

Amendment context."[165] Most importantly, "Fourth Amendment protections for your papers and effects do not automatically disappear just because you share them with third parties."[166]

Justice Gorsuch realized the prominent effect *Katz* has had on Fourth Amendment jurisprudence and that courts would need help to reapply the traditional approach to the Fourth Amendment. However, he acknowledged that more work is needed to resuscitate this area of law before his theory could be fully implemented, and thus offered multiple thoughts for guidance.[167] One of his chief thoughts was his proposal to use bailments as a way of addressing third-party doctrine issues.[168]

"A bailment is the 'delivery of personal property by one person (the bailor) to another (the bailee) who holds the property for a certain purpose."[169] A bailee has a legal obligation to keep the item or thing safe, and to use it in accordance with the agreed upon intended purpose, or otherwise the bailee could face legal consequences.[170] Justice Gorsuch cements his theory of bailments in the traditional Fourth Amendment precedent of *Ex parte Jackson*,[171] where the Court wrote: "The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be."[172] Justice Gorsuch also opined that "[j]ust because you entrust your data—in some cases, your modern-day papers and effects—to a third party may not mean you lose any Fourth Amendment interest in its contents."[173] Justice Gorsuch provides a foundation on which this

165. *See id.* at 2268.

166. *Id.*

167. *See id.* at 2268–71.

168. *Id.* at 2268–69.

169. *Id.* at 2268 (quoting *Bailment*, BLACK'S LAW DICTIONARY (10th ed. 2014)) (citing JOSEPH STORY, COMMENTARIES ON THE LAW OF BAILMENTS, § 2, at 2 (1832)).

170. *See id.* at 2268–69.

171. 96 U.S. 727 (1878). This Court held that sealed letters placed in the mail are "as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles." *Id.* at 733.

172. *Id.*

173. *Carpenter*, 138 S. Ct. at 2269. An example of a bailment would be when an individual gives his car keys to a valet at a restaurant; that individual

Comment builds its theory of the "adhesion bailment." The "adhesion bailment doctrine" is premised on fairness and provides enhanced protection to the individual IoT user. Courts can use bailments as a way to clarify what privacy protection an IoT user maintains.

There are two ways one can view a service provider as a bailee.[174] The first is viewing a third-party company as an intermediary, i.e., a bailee, who is provided the information to perform a task, rather than as the "recipient" of the information. For example, when one uses an IoT device such as an Amazon Echo and asks it to send an email, Amazon, the third-party company, is not the recipient of that information. The IoT user is "voluntarily" sending that information to Amazon, and even though Amazon may store the information for business purposes, Amazon's main function is to take that information and deliver it to the actual intended recipient. Thus, just as a mail carrier cannot consent to the disclosure of the contents of the letter she is delivering, Amazon cannot consent to the disclosure of the contents of the email. Furthermore, the government's argument that the IoT user does not have exclusive control or complete ownership over the information should be rejected. If anything, the opposite principle is reflected in American jurisprudence, as tenants who rent an apartment and family members who do not own legal title to their home "still have standing to complain about searches of the houses in which they live."[175] Therefore, IoT users who voluntarily provide data to a third-party company as a bailee, or in an intermediary capacity, should maintain Fourth Amendment protection in that information.

The second way to view a third-party company as a bailee is through the proposed "adhesion bailment doctrine."[176] This doctrine provides greater protection to the IoT user than the current regime and is premised on inherent fairness. As noted above, society is coming to a point where the IoT will constantly gather data on all individuals. By merely living in an IoT world,

---

knows that he will get his keys and vehicle back at the end of his meal. *Id.* at 2268.

174. *See id.* at 2268–69. This paragraph draws from Justice Gorsuch's theory on bailments and applies it practically in the IoT world.

175. *Id.* at 2269–70.

176. The "adhesion bailment doctrine" is based on this author's own theory.

one is continuously providing data to a third party; it is difficult to understand how anyone can honestly state that such information is voluntarily conveyed. The third-party doctrine is predicated on an individual voluntarily providing information to another. Accordingly, the "adhesion bailment doctrine" is triggered when a third-party company collects data on individuals through means of the user's day-to-day activities—essentially, the user will automatically have Fourth Amendment protection in the information third-party companies collect through the user's daily routine. The fact that the information collected from third-party companies from IoT users is not voluntarily disclosed is the central part of the reasoning why the term "adhesion" is used in this doctrine's name. Thus, regardless of how advanced technology becomes, the user's privacy rights will always remain intact.

For example, in the IoT, the government could obtain a subpoena for the records of a conversation an individual had while sitting in front of his television at home, not realizing the TV was recording him. The government could also obtain one's conversations and whereabouts while driving a vehicle because many cars have emergency communications hardware installed, similar to OnStar technology. In more advanced cities, sensors are placed in many objects, such as recycling bins. As one passes by, the sensor can track the Wi-Fi signals from passing phones, giving the government an individual's location at any given time. These examples highlight only a few ways the government can use the IoT to investigate individuals. If courts followed the "adhesion bailment doctrine," any attempt by the government to obtain the type of data described would trigger Fourth Amendment protection to the IoT user. Therefore, the government would have to establish probable cause and either obtain a warrant or show a recognized exception to the warrant requirement to receive any information stored with the third-party companies. This solution provides ample protection to the IoT user by prohibiting the government from using the current interpretation of the third-party doctrine to obtain sensitive personal information without probable cause—the standard required according to the Constitution.[177]

177. U.S. CONST. amend. IV ("[N]o Warrants shall issue, but upon probable cause . . . .").

CONCLUSION

Federal law and jurisprudence regarding digital privacy has not responded to advancements in technology quickly enough. Although some state legislatures have attempted to create more privacy protection for individuals, those laws are still lacking, and more importantly, they only protect the individuals of the respective state. Additionally, current legislation and common law are continuing to provide the government with backdoor access around an individual's Fourth Amendment protection through the use of the third-party doctrine. Nevertheless, if the third-party doctrine is abandoned, it will likely be replaced with something that is more complicated, or at least more nuanced, than its predecessor. Thus, until workable law is created that will balance the need of government investigation and individual privacy protection of digital data, the third-party doctrine will remain. Accordingly, this Comment's proposed doctrine of adhesion bailments provides protection to the individual IoT user, and at the same time, does not alter the interpretation of the third-party doctrine. Although the government will not have the power it currently possesses in the digital age, it can still use the third-party doctrine in limited respects, creating a workable balance between governmental intrusion and protection of individual privacy. Of course, the government can continue to conduct investigations as it has prior to the advancement of technology—through adherence to the Fourth Amendment. However, even though this Comment proposes a way of maintaining an individual's privacy rights in the digital age, the overwhelming theme is that technology is always advancing. Today witnesses the IoT, tomorrow might see artificial intelligence, and what else the future holds, no one knows. Thus, the Fourth Amendment must be adaptable to an ever-changing society.