# REASONABLE EXPECTATIONS OF PRIVACY IN THE DIGITAL AGE

*Jessica F. Silva**



## I. INTRODUCTION

In its entirety, the Fourth Amendment reads:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[1]

Congress passed the Fourth Amendment ("the Amendment") on September



* J.D. Candidate, 2020, Seton Hall University School of Law; B.A. in Political Science and Business Administration, *cum laude*, 2017, Seton Hall University. I would like to give a special thanks to my family for their endless love, support, and encouragement in all of my endeavors.

[1] U.S. CONST. amend. IV.

25, 1789, and it was subsequently ratified on December 15, 1791.[2] When it was written over two hundred years ago, the writers intended for the Amendment to provide exactly what it said— protection for citizens from unlawful searches and seizures absent a warrant or probable cause.[3] At the time the Fourth Amendment became part of the Constitution, it was only intended to be applied to the federal government; later, however, the Amendment became applicable to the states through the Due Process Clause of the Fourteenth Amendment.[4]

Interpretation of the Fourth Amendment can be split into two ideologies: original intent and original meaning.[5] Proponents of the first ideology would look at the constitutional framer's understanding when they wrote the Amendment.[6] In other words, advocates of original intent see the Amendment as covering exactly what the framers wrote at the time; therefore, the Fourth Amendment would not cover devices—such as cell phones—that did not exist in the eighteenth century.[7] On the contrary, proponents of original meaning ask what a reasonable person would interpret the meaning of the Amendment to be at the time of its ratification.[8] Proponents of this theory look at the Amendment as ever-changing to provide protections consistent with the needs of the era—meaning that the connotation of the Amendment from the time of ratification (a guarantee from unreasonable searches and seizures) remains exactly the same, however, the definition of those domains protected by the Amendment (persons, houses, papers, and effects) are apt for a change of interpretation.[9]

Whether a search is reasonable in the eyes of the law is determined by balancing two interests: (1) intrusion on the Fourth Amendment rights of the individual; and (2) legitimate government interests such as public safety.[10] In recognizing this, American jurisprudence has created exceptions to the Fourth Amendment warrant requirement that respect these two interests.[11]

---

2 *Id.*

3 Olmstead v. United States, 277 U.S. 438, 463 (1928) ("The well-known historical purpose of the Fourth Amendment, directed against general warrants and writs of assistance, was to prevent the use of governmental force to search a man's house, his person, his papers and his effects; and to prevent their seizure against his will."); *see also* U.S. CONST. amend. IV.

4 Mapp v. Ohio, 367 U.S. 643, 655 (1961).

5 Thomas B. Colby & Peter J. Smith, *Living Originalism*, 59 DUKE L.J. 239, 250 (2009).

6 *Id.* at 248.

7 *See generally* Colby & Smith*, supra* note 5, at 248.

8 Colby, *supra* note 5, at 250.

9 *See id.* at 250–53.

10 Delaware v. Prouse, 440 U.S. 648, 654 (1979).

11 *See id.* An example of this would be a vehicle search by an officer during a traffic stop—but only with probable cause.

Applying the Fourth Amendment as it pertains to today's digital age from an original intent standpoint presents many challenges; application of this ideology suggests that one's electronic devices are not shielded from unlawful searches and seizures without a warrant or probable cause.[12] Modern interpretation of the Fourth Amendment leads to a peculiar issue—what is covered by the Fourth Amendment in the modern era? For the purposes of this paper, an original meaning stance will be taken to explore the issue of whether or not the Fourth Amendment has effectively adjusted to the digital age. A cell phone search can reveal as much about an individual as the search of a home, yet some courts have deemed warrantless cell phone searches constitutional.[13] Thus, if a search of a cell phone is as invasive as that of a home, it stands to reason the same guidelines should apply when determining what constitutional protections are applicable. Furthermore, an individual's digital trail can be stitched together to paint a picture of his or her private life.[14] The protections afforded to one's "papers and effects" are a matter of privacy and if digital trails assist in taking away privacy, then they should be afforded protection under the Fourth Amendment.

In an age where much of an individual's life is centered around electronic devices, what is protected from unreasonable search and seizure by the Fourth Amendment? In other words, what constitutes "papers and effects"? The definition of "papers and effects" depends on an interpretation of what one can reasonably expect to be private.[15] Do internet searches, cell phones, data stored in the "cloud," emails, and all other aspects of one's digital footprint fall under the blanket of protection the Constitution's framers meant for citizens when writing the Fourth Amendment? Under current law, these activities are given very little privacy protection, undermining constitutional safeguards that are essential to individual liberties and a robust democracy.[16] This creates a privacy gap by denying Fourth Amendment protection to data processed by third parties, including data stored in the "cloud."[17]

---

12 *See generally Colby* & Smith, *supra* note 5, at 250.

13 *See* Riley v. California, 573 U.S. 373, 396–97 (2014) ("[A] cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is."); *see also* United States v. Carpenter, 819 F.3d 880, 888 (6th Cir. 2016); United States v. Jones, 565 U.S. 400 (2012).

14 *See Riley*, 573 U.S. at 396–97.

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

16 Michael W. Price, *Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine*, 8 J. NAT'L SECURITY L. & POL'Y 247, 247 (2016).

17 *Id.*

The issue at hand is whether the "reasonable expectation of privacy" test attributed to the Fourth Amendment adequately protects privacy interests in today's digital age. As time progresses and technology advances, the privacy gap has widened and no measures have been taken to fill the void. The laws governing online privacy are older than the internet and the laws in place protecting electronic communications are an inconsistent and illogical patchwork.[18] In the digital age, the standard "reasonable expectation of privacy" test attributed to the Fourth Amendment is outdated. The present test does not adequately protect digital communications and a different test is needed for digital communications, which the Electronic Communications Privacy Act of 1986 ("ECPA") should be updated to include.[19]

This comment argues for the need for a distinct test for digital privacy protections accounting for the changes brought on by modern technology, which the ECPA should be amended to include. Part II of this comment delves into the origins of digital privacy protections. Part III critiques protections in place today, dissecting the fatal flaw in applying outdated mechanisms. This section also analyzes what makes digital content different and how digital privacy rights can be secured through amendment of the ECPA. Finally, part IV concludes that technological developments have put a tremendous amount of stress on the antiquated Fourth Amendment privacy protections of today and that a new framework for digital content should be implemented through the ECPA.

## II. A LOOK AT THE HISTORY OF DIGITAL PRIVACY

### *A. Katz v. United States*

The springboard for digital privacy came in 1967 with *Katz v. United States*.[20] Here, the petitioner, Katz, had been convicted of transmitting gambling information over the telephone.[21] To acquire the information that led to Katz's conviction, the federal agents investigating him attached an eavesdropping device outside the public phone booth used by Katz; at trial, the recordings of Katz's conversations were entered into evidence to be used against him.[22] The question presented in this case became whether the Fourth Amendment's "unreasonable searches and seizures" protection required police to obtain a search warrant before wiretapping a public

---

[18] *Id.*

[19] *See* Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. §§ 2510–23 (2018).

[20] *See generally Katz*, 389 U.S. 347.

[21] *Id.* at 348.

[22] *Id.*

payphone.[23] The Court ruled that the government's use of an electronic device to record conversations inside a telephone booth without a warrant was a violation of the Fourth Amendment.[24] *Katz* declared that the Fourth Amendment "protects people, not places"; this was a dramatic shift in reasoning from previous rulings of the Court, which had been dominated by the concepts of property and trespass.[25] Although Katz had been having a conversation in a public telephone booth, he sought to preserve the conversation as private—as demonstrated by his shutting of the booth door behind him; the government's eavesdropping violated the privacy "upon which he justifiably relied."[26]

Out of this case came the "reasonable expectation of privacy" formula, commonly referred to as the *Katz* test.[27] The test is based on the concurrence of Justice John Harlan in the case, in which he stated, "[m]y understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person has exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable'"[28]

This test has become the balancing test of Fourth Amendment protection in many cases, particularly those involving electronic surveillance.[29] Theoretically, this rule is reasonable because it would appear on the surface to help adapt Fourth Amendment protections to the evolving digital age. However, the discretion is all in the hands of judges to determine if an individual truly expected privacy in a given situation, and then to decide whether society is prepared to accept that expectation as reasonable.[30] New York University Law professor, Anthony Amsterdam, discusses the inquiries into the reasonable expectation test, calling them "needless," maintaining that the inquiry into what society expects to be private "destroys the spirit of *Katz* and most of *Katz*'s substance."[31] Amsterdam goes on to note the government could quite easily weaken our expectations of privacy by "announcing half-hourly on television that . . . we were all forthwith being placed under comprehensive electronic surveillance."[32] Amsterdam further expounds upon the idea that the government can effortlessly

---

[23] *Id.* at 349–50.

[24] *Id.* at 359.

[25] *Katz*, 389 U.S. at 351.

[26] *Id.* at 353.

[27] Price, *supra* note 16, at 249.

[28] *Katz*, 389 U.S at 361 (Harlan, J., concurring); *see also* Price, *supra* note 16, at 261.

[29] Price, *supra* note 16, at 262.

[30] *Id*.

[31] Anthony Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 383 (1974).

[32] *Id.* at 384.

overcome privacy expectations, noting that expectations are shaped by what practices the law allows—making the *Katz* test somewhat circular.[33]

While the test may have been workable enough in the era of its conception, applying the test to the modern era has weakened privacy interests.[34] This issue will only worsen as time goes on if the test continues to be used in the digital era.[35] Courts are unable to balance privacy interests against those of law enforcement, and as technology continues to advance, areas in which a person can reasonably expect privacy will decrease until this expectation becomes virtually non-existent.[36]

*B. "Reasonable" Expectations of Privacy*

The core policy concerns underlying the Fourth Amendment are the individual privacy expectations that individuals must possess for society to be free and functional.[37] The problem with this statement, however, is it has not been made clear how this societal expectation should be measured. One measurement for gauging reasonable privacy expectations is by "assessing the frequency of public traffic in an area"—in other words, if an activity is occurring in a public area with a high chance of discovery or observation, society should not accept a claim to privacy as valid or reasonable.[38]

In looking at privacy expectations in the modern era, one can look to the relatively recent case of *United States v. Jones*.[39] In *Jones*, the Court stepped away from the *Katz* standard and headed down a different privacy path. This case dealt with a respondent who was under suspicion of narcotics trafficking.[40] Authorities were granted a warrant authorizing them to put a Global Positioning System ("GPS") tracking device on the underside of Jones' vehicle; they did so, however, after the deadline stated on the warrant.[41] Using the GPS device they had unconstitutionally installed, the officers tracked the vehicle's movements and eventually obtained an indictment against the accused, which included charges of conspiracy to distribute cocaine.[42] The question posited in *Jones* was whether the

33 Price, *supra* note 16, at 262.

34 *Id.*

35 *Id.*

36 Brandon T. Crowther, *(Un)Reasonable Expectation of Digital Privacy*, 2012 BYU L. REV. 343, 344 (2012).

37 Courtney E. Walsh, *Surveillance Technology and the Loss of Something a Lot Like Privacy: An Examination of the "Mosaic Theory" and the Limits of the Fourth Amendment*, 24 ST. THOMAS L. REV. 169, 187 (2012).

38 *Id.* at 188.

39 *See generally* United States v. Jones, 565 U.S. 400 (2012).

40 *Id*. at 402.

41 *Id.* at 400.

42 *Id.* at 403.

attachment of the GPS device to the respondent's vehicle and its use to monitor the movements of the vehicle constituted a "search and seizure" as it pertains to the Fourth Amendment.[43]

The ruling passed down in *Jones* stated, unanimously, that the installation of a GPS tracking device underneath Jones' car qualified as a search under the Fourth Amendment.[44] It might be presumed that the Court came to this conclusion through the application of the *Katz* test[45]; however, in this instance the Court switched gears, instead applying a trespass doctrine from the 1928 case *Olmstead v. United States*.[46] Due to what the Court called a "physical intrusion"—the means by which the officers accessed the vehicle to attach the device[47]—the Court chose to abandon *Katz* in this instance.[48] Because of the nation's incessant reliance on technology as a form of communication, a reasonable theory is that Scalia felt society's expectation of privacy was eroding.[49] With today's heavy reliance on social media as a form of interaction, the lines of what privacy rights citizens consider "reasonable" become blurred. *Katz* cannot provide the Fourth Amendment protection it was intended any longer.

### *C. The Electronic Communications Privacy Act*

Because many forms of communication were not properly protected, Congress implemented the ECPA in 1986 in an effort to keep up with new technologies.[50] The ECPA governs prohibitions on the interception of electronic communications.[51] The ECPA prohibitions relate to "any wire, radio, electromagnetic, photo-optical or photo-electronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications."[52] *Katz* stands for the idea that no Fourth Amendment protection exists without a reasonable expectation of privacy.[53] If there is no reasonable expectation of privacy, then there is no violation of a Fourth

---

43 *Id.* at 402.

44 *Id.* at 404.

45 Because *Katz* was the usual test for Fourth Amendment protection in these types of cases.

46 Brian M. Kistner, *The Fourth Amendment in the Digital World: Do You Have an Expectation of Privacy on the Internet?*, Seton Hall Law School Student Scholarship 1, 10 (2016); *see also* Olmstead v. United States, 277 U.S. 438 (1928).

47 The officers encroached on private property to access the vehicle.

48 *Jones*, 565 U.S. at 400.

49 Kistner, *supra* note 46, at 11.

50 1-2 Law of The Internet § 2.03(4)(a) (2017).

51 18 U.S.C. §§ 2510–23.

52 18 U.S.C. § 2510(14).

53 *See generally Katz*, 389 U.S. at 347.

Amendment right for a claim based on the ECPA.[54] While the ECPA granted protection to previously unprotected forms of electronic communication, the legislation still leaves something to be desired.

When the ECPA was enacted, its creators did not foresee the technological society we live in today. Its provisions were meant to deal with government intrusions by technology of the time, which has grown to be worlds apart from that which exists today.[55] The immense amount of data that technology is capable of collecting creates far greater implications for Fourth Amendment protections than the ECPA writers could have possibly imagined.[56] Present protections fall flat—data is and should be recognized as fundamentally distinct. As the ECPA exists today, courts are left to attempt to apply provisions meant for traditional surveillance methods to digital searches.

*D. Another Layer: Mosaic Theory*

*United States v. Maynard*, decided in 2010, held the government's warrantless surveillance of a defendant via a GPS device mounted on his car for over a month violated the Constitution's protection against warrantless searches.[57] The striking similarity to the *Jones* case is to be noted; the court in *Maynard* stepped away from the Fourth Amendment jurisprudence of the time—just like in the *Jones* ruling.[58] To reach their ruling, however, the *Maynard* court used what is known as the mosaic theory and adapted it to the context of the Fourth Amendment.[59] Under this "mosaic theory of privacy," while individual actions of law enforcement may not be considered searches for Fourth Amendment purposes, when taken together they may be considered searches.[60] Prior to *Jones*, decisions regarding the Fourth Amendment had always broken down each part of an investigation individually.[61] GPS surveillance decisions could indicate the Court is ready to embrace a new mosaic theory of Fourth Amendment protection.

---

54 1-2 Law of The Internet § 2.03(2) (2017).

55 *See* Jennifer Arner, *Looking Forward By Looking Backward: United States v. Jones Predicts Fourth Amendment Property Rights Protections in E-mail*, 24 GEO. MASON U. CIV. RTS. L.J. 349, 360.

56 *See id.*

57 *See generally* United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010).

58 *Compare id.* at 559–61 (surveying recent Fourth Amendment jurisprudence), *with Jones*, 565 U.S. at 405 (noting the Court's shift in Fourth Amendment jurisprudence after 1967).

59 *Maynard*, 615 F.3d at 562; *see also* Erin Smith Dennis, *A Mosaic Shield: Maynard, the Fourth Amendment, and Privacy Rights in the Digital Age*, 33 CARDOZO L. REV. 737, 738 (2011).

60 Dennis, *supra* note 59, at 738.

61 Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 312 (2012).

What sets the mosaic theory apart from traditional Fourth Amendment search doctrine is that it looks at government conduct as a whole rather than as individual steps.[62] The mosaic theory looks at whether non-searches, when analyzed in the aggregate, are so revealing they amount to a search.[63]

## III: CRITICISMS OF TODAY'S DIGITAL PRIVACY PROTECTIONS

### *A. Criticism of Katz*

The standard "reasonable expectation of privacy" test attributed to Fourth Amendment searches dates back to Justice John Harlan's concurrence in *Katz v. United States*.[64] The binary requirement of the test is that "a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[65] The requirements set forth make sense logically, but each is not without its own issues when applied to the modern digital context.

The first prong of *Katz* requires that there be a subjective interest of privacy to establish a legitimate privacy interest.[66] The policy rationale behind this is that there is no reason why a right of privacy should be granted to an individual who does not have an actual expectation of privacy.[67] The problem with this rationale is that it is difficult to determine whether an individual has a subjective expectation of privacy. The Supreme Court has not been able to provide much guidance on this standard because it is unavoidably fact intensive. The only insight the Court has provided is that an individual must outwardly show in some way that he seeks to preserve something as private, essentially applying an objective measurement to this subjective prong.[68] For an individual to have an expectation of privacy, the external evidence must show he sought to protect something as private through his conduct.[69] On the other hand, searches involving any sort of tangible object generally question whether the object is physically locked.[70] In a majority of cases, the subjective prong becomes inapt because it adds little to analysis.[71] As expectation of privacy is a subjective concept, it is difficult to ascertain whether it exists or not. Adding to this difficulty is the

---

62 *Id.* at 320.

63 *Id.*

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

65 *Id.*

66 *Id.*

67 Crowther, *supra* note 36, at 346.

68 *Id.*

69 Mary Graw Leary, *Reasonable Expectations of Privacy for Youth in a Digital Age*, 80 MISS. L.J. 1033, 1057 (2011).

70 Crowther, *supra* note 36, at 346.

71 *Id.* at 346–47.

fact that often times even if a person were to have a subjective expectation of privacy, society would not recognize it as reasonable.[72] The legitimacy of the subjective prong relies upon accurately determining one's mental state to judge whether he actually expects privacy, which is exceedingly difficult.[73]

The second prong of *Katz* relies upon society's objective expectations.[74] Much like judging one's subjective expectation of privacy, deducing what privacy expectations society is willing to accept as reasonable is an arduous task. The Supreme Court fails to articulate a clear objective standard to measure society's expectations, saying only that judges should look at "widely shared societal expectations" and giving no guidance as to how one should go about determining that shared expectation.[75]

This prong of *Katz* has become an exceedingly flexible one—ultimately leaving what "society" is willing to recognize as reasonable up to one person—a judge. This leads to inconsistent applications of the standard, which impedes the fundamental privacy interest. These contentions are not without merit—even the Supreme Court has voiced its concern over *Katz* as a proper measure of Fourth Amendment coverage.[76] In the 2010 case of *City of Ontario v. Quon*, the Court's confidence in *Katz* was put to the test.[77] The issue in *Quon* involved a police department supervisor's searching of an officer's private messages on an electronic mobile device that had been issued to the officer for use in his work.[78] This search was not for nefarious purposes, but rather, because Mr. Quon had repeatedly gone over his message limit and the supervisor sought to determine whether the overage was for personal or work-related messages.[79] The city of Ontario reserved the right through its "Computer Usage, Internet, and E-Mail Policy" to audit the messages, however, they contended they would not do so if the employee paid for overage—which Quon had done.[80] The officer brought a Fourth Amendment claim against the city; applying *Katz* to the issue at hand, the Court was to evaluate society's privacy expectations of text messages sent and received on an employer's electronic mobile device.[81] The justices in the case took issue with applying *Katz* to the case in assessing the privacy interest; they did not see a correlation between the privacy interest in a

---

72 *Id.* at 347.

73 *Id.*

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

75 Crowther, *supra* note 36, at 348; *see also* Georgia v. Randolph, 547 U.S. 103, 129 (2006).

76 *See* City of Ontario v. Quon, 560 U.S. 746, 759 (2010).

77 *Id.* at 746.

78 *Id*.

79 *Id.* at 752.

80 *Id.* at 751–52.

81 *Quon*, 560 U.S. at 750.

telephone booth and that of texting at the office, as the two are worlds apart.[82] In the end, the Court decided that even if this surveillance constituted a search, it was reasonable—therefore, the City of Ontario did not violate Mr. Quon's Fourth Amendment rights.[83] Applied to the modern era, it has become evident that the *Katz* test has faced a plethora of issues with regard to its application to digital content.[84]

*B. What makes digital content different?*

It has become remarkably difficult to mechanically apply the *Katz* reasonable expectation of privacy test because digital content inherently differs on many levels from that which *Katz* was originally applied to.[85] Digital content pervades virtually every facet of American life, creating a mass amount of digital information which only continues to grow larger.[86] It differs from physical data in its quantity, quality, and permanence, among other things. Information which was previously physical is now being converted to digital form, and computer technology has made it so the number of files, images, and documents one can create in the digital sphere is seemingly endless.[87] Adding to this is the fact that computers often record information unbeknownst to the user—an individual's internet history is recorded on his hard drive, constructing a trail of what has been done on that computer.[88] Additionally, the permanence of evolving digital technology has changed the meaning of "privacy." As so much information and history are conserved online, it can be easily accessed and collected by the government in mass quantities.

Perhaps the most drastic way that digital data differs from physical data is the quantity of information that can be obtained digitally. A physical search of a home, for example, will only turn up so much digital information due to its capacity. Conversely, a computer has a seemingly endless capacity, with the ability to hold up to terabytes of data.[89] A digital search, therefore, is intrinsically different than a physical search because it gives access to massive amounts of information which could not possibly be obtained through a physical search.

---

82 *Id.* at 761.

83 *Id.* at 765.

84 *See, e.g., Quon*, 560 U.S. 746.

85 *See generally Katz*, 389 U.S. 347. The test, when used in *Katz*, involved the use of a listening device on the outside of a telephone booth and whether the defendant's Fourth Amendment right to privacy had been violated.

86 Scott D. Blake, *Let's Be Reasonable: Fourth Amendment Principles in the Digital Age*, 5 SEVENTH CIR. REV. 491, 499 (2010).

87 *Id.*

88 *Id.*

89 *Data, Data Everywhere*, THE ECONOMIST, Feb. 27, 2010 (last accessed April 2, 2020).

With digital data differing in quantity, quality, and permanence from the traditional physical data that the courts have been accustomed to dealing with, the question then becomes how digital data should be treated with respect to the Fourth Amendment. In this sense, the *Katz* reasonable expectation of privacy test must be revaluated with respect to digital searches, as digital data should be protected just as efficiently as tangible objects.

The technological developments of today have placed a tremendous amount of stress on the frameworks for Fourth Amendment privacy protections. These protections developed in an era when electronics did not exist or otherwise were not prevalent, and the Supreme Court has been unsuccessful in keeping up with the application of the Fourth Amendment with today's technology.

### *C. Mosaic Theory Issues*

The mosaic theory presents a new challenge to settled law.[90] The mosaic theory is premised on aggregation and takes re-evaluation of settled law in a substantially different direction.[91] In light of new surveillance technologies, such as real-time GPS surveillance, the United States Court for the District of Columbia took what was then a conceptually new approach to Fourth Amendment law in the case of *United States v. Maynard*.[92] This new "mosaic theory" approach sought to foster a constitutionally anchored "sphere of privacy" which would come into play under situations of long-term, technology driven investigations.[93] This set the approach apart from the mechanically applied *Katz* test in the sense that it generally provides a greater affordance of privacy to the monitored individual.[94] The premise of the mosaic theory is that while a set of non-searches taken separately may be considered exactly that (non-searches), if the data taken in aggregate can create a mosaic which reveals essentially private insights about an individual, it will trigger Fourth Amendment scrutiny.[95]

#### 1. *United States v. Maynard and United States v. Jones*

To understand the mosaic theory, one must first look to the cases of *United States v. Maynard* and *United States v. Jones*—these were separate cases dealing with the same issue.[96] In *Maynard* and *Jones*, the respondents

90 Kerr, *supra* note 61, at 314.
91 *Id.*
92 Walsh, *supra* note 37, at 173.
93 *Id.*
94 *Id.*
95 *See* Kerr, *supra* note 61, at 313.
96 *Maynard*, 615 F.3d at 544; *see also Jones*, 565 U.S. at 400.

were under the suspicion of narcotics trafficking; following a two-year investigation, it was discovered that the two men (Jones and Maynard) ran a "stash house"—the contents of which included ninety-seven kilograms of cocaine, one kilogram of crack, and $850,000 in cash.[97] However, what is of primary importance here is not the results of the investigation, but the investigative techniques that lead to its culmination.

To begin, Jones and Maynard were put under visual surveillance.[98] If an activity is being conducted in a public area with a high chance of discovery or observation, it is suggested that society should not accept a claim to privacy as valid or reasonable—so, per the *Katz* test, this is not a search.[99]

The second method used by the investigators goes a bit farther than the aforementioned, and involved the tracking of the suspects' cell phones.[100] Here, the investigators applied for and obtained court orders which compelled Jones' cellular provider to release the cell tower information for Mr. Jones' phone.[101] Cell phones function through connection to local cell towers, which in turn route communications.[102] As such, cell phone providers keep records of which towers were used by which account.[103] Most individuals tend to carry their cell phones with them, and consequently these cell phone records act as a tracking device.[104]

The third method used by authorities was to obtain a warrant authorizing law enforcement to put a GPS tracking device on the underside of Jones' vehicle.[105] They did so, however, one day after the deadline stated on the warrant.[106] This method is where a bulk of the *Maynard* and *Jones* cases focused.[107] Using the GPS device they had unconstitutionally installed, the officers tracked the vehicle's movements and eventually obtained an indictment against the accused.[108] The question posited in *Maynard* and *Jones* was whether the attachment of the GPS device to the respondents' vehicle and its use to monitor the movements of the vehicle constituted a

---

97 *Maynard*, 615 F.3d at 548, 567; *see also Jones*, 565 U.S. at 404.

98 *Id.* at 549.

99 Walsh, *supra* note 37, at 188.

100 *Maynard*, 615 F.3d at 549.

101 *Id*.

102 Steven M. Harkins, *CSLI Disclosure: Why Probable Cause Is Necessary to Protect What's Left of the Fourth Amendment*, 68 WASH. & LEE L. REV. 1875, 1877 (2011).

103 *See, e.g.,* In re Application of the United States for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013).

104 Kerr, *supra* note 61, at 322.

105 *Maynard,* 615 F.3d at 555; *see also Jones*, 565 U.S. at 400.

106 *Id*. Because the device was installed after the deadline stated on the warrant, the use of the GPS device on the vehicle was warrantless.

107 *See Maynard*, 615 F.3d at 544; *see also Jones*, 565 U.S. 400.

108 *Id*.

search and seizure as it pertains to the Fourth Amendment.[109]

The ruling passed down in *Jones* states unanimously that the installation of a GPS tracking device underneath Jones' car qualified as a search under the Fourth Amendment.[110] It might be presumed the court came to this conclusion through the application of the *Katz* test, however, this is where the mosaic theory came into play.

The prosecution attempted to admit the GPS evidence the authorities on the case collected to show that Jones was involved, however, Jones moved to suppress it.[111] The Court determined any evidence indicating the car was in Jones' garage had been obtained in violation of the Fourth Amendment; this was an area that it can be posited that Jones had a reasonable expectation of privacy.[112] However, the judge, citing *United States v. Knotts*, decided that the same analysis applied to GPS monitoring.[113] Both Maynard and Jones were convicted and both appealed their convictions, however, only Jones challenged the GPS evidence allowed at trial.[114]

Jones argued on appeal that *Knotts* should not be applicable because comparing a GPS device to a beeper was an invalid comparison technology-wise; GPS tracking is far more advanced.[115] This is where the mosaic theory argument came into play: the GPS device, when all the information it collected was pieced together, collected so much data that it created an exceptionally clear picture of the defendant's life.[116] This monitoring was so intrusive it bore resemblance to an invasive search.[117] This argument convinced the Court to overturn Jones' conviction on the grounds that the use of the GPS device over twenty-eight days was a Fourth Amendment search.[118] In the court's view, the monitoring of the GPS over time constituted a search because while, indeed, the public could observe Jones' individual movements, it was highly improbable the public would observe

109 *Id.*

110 *Id.*

111 *Id.*

112 *Maynard*, 615 F.3d at 563–64.

113 *Id.* at 555–56 (citing United States v. Knotts, 460 U.S. 276 (1983) (explaining that a person traveling on a public road has no reasonable expectation of privacy, and therefore the use of a beeper positioned in a suspect's car by authorities to broadcast location was permissible)).

114 *See Maynard*, 615 F.3d at 544; *see also Jones*, 565 U.S. 400.

115 *Maynard*, 615 F.3d at 556.

116 *Id.* at 562; *see* People v. Weaver, 909 N.E.2d 1195, 1199 (N.Y. 2009) (determining that prolonged GPS monitoring yields a highly detailed profile beyond just location, but also of our associations and patterns); *see also* State v. Jackson, 76 P.3d 217, 224 (Wash. 2003) (en banc) (stating that GPS tracking devices record travels and can be used to paint a detailed picture of one's life).

117 *See* United States v. Jones, 565 U.S. 400, 417 (2012).

118 *Maynard*, 615 F.3d at 568.

the complete set of his movements that the GPS device revealed.[119] The tracking painted an alarmingly clear picture of Jones' life that he would not expect others to have.[120] Although there were concurring opinions in *Maynard* and *Jones*, the opinions all agreed on one thing—that it was the collective sum of government action, not individual sequential steps, which are to be looked at when determining what counts as a Fourth Amendment search.[121]

The *Jones* ruling may have reinforced Fourth Amendment rights as they pertain to GPS, but with technology constantly evolving it is impossible to say for how long the ruling will remain relevant.[122] The third-party doctrine, or the idea that when one consents to releasing data to at least one third party (such as a cell phone provider) they have no reasonable expectation of their data being private, plays an incredibly large role in this.[123] Physical contact no longer needs to be made in order to use GPS to track an individual; cell phone based GPS as well as programs integrated into vehicles (such as the Ford Sync or OnStar) make one's GPS data property of a third-party, and as such can be obtained by law enforcement.[124]

2. Third-Party Doctrine

The third-party doctrine is the Fourth Amendment rule which dictates that an individual gives up all Fourth Amendment protections with regard to the information disclosed to a third-party.[125] Any assumption of purpose or confidence in the third party on the part of the revealing individual is irrelevant.[126] Therefore, *Katz* does not apply, as an individual cannot have a reasonable expectation of privacy in information disclosed to a third party.[127]

Critics of the doctrine make two arguments.[128] The first criticism is that the doctrine does not accurately apply the *Katz* reasonable expectation of privacy test.[129] Indeed, individuals generally expect privacy with respect to third-party records such as phone records.[130] Justice Marshall's reasoning in

119 *Id.* at 558.

120 *See id.*

121 *See Maynard*, 615 F.3d 544; *see also Jones*, 565 U.S. at 400.

122 *See generally Jones*, 565 U.S. at 400.

123 *See* Price, *supra* note 16, at 277.

124 *See id.* at 291–92.

125 Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 528–29 (2006).

126 *Id.* at 529.

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

128 *See* United States v. White, 401 U.S. 745 (1971); *see also* Joseph E. Schumacher & Christopher Slobogin, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society*," 42 DUKE L.J. 727, 732 (1993).

129 Schumacher & Slobogin, *supra* note 128, at 732.

130 Gerald G. Ashdown, *The Fourth Amendment and the "Legitimate Expectation of*

his *Smith v. Maryland* dissent reflects the same.[131] It is difficult to reason that an individual "voluntarily" surrenders information to a third party such as a telephone company—they have no choice in the matter.[132] The second argument critics of the doctrine make is that it grants government too much power—it gives government the authority to take more intrusive steps without constitutional oversight than is consistent with societal freedoms and expectations.[133] This argument contends the government is given the power to, essentially, harass individuals.[134] The major concern proponents of this argument have is that because third-party services such as Internet Service Providers and phone providers are so prevalent in today's digital age, if these services take a growing role in government surveillance, the Fourth Amendment will regulate less digital surveillance.[135] If the Fourth Amendment is not protecting third-party service, the government can collect more information that one might "reasonably" expect to be private from Fourth Amendment scrutiny.[136]

*D. Securing Privacy Rights*

> In Justice Samuel Alito's concurrence in *Riley v. California*, he argued:
>
> We should not mechanically apply the rule used in the predigital era to the search of a cell phone. Many cell phones now in use are capable of storing and accessing a quantity of information, some highly personal, that no person would ever have had on his person in hard-copy form.

Justice Alito further suggested that Congress or state legislatures consider new laws that draw rational divisions based on categories of information, otherwise privacy protection in the twenty-first century will suffer.[137]

The best body to deal with the issue of privacy concerns with respect to electronic surveillance is the legislature; courts are reactive, but it is the

*Privacy*," 34 VAND. L. REV. 1289, 1315 (1981).

131 Smith v. Maryland, 442 U.S. 735, 750 (1979) (Marshall, J., dissenting) (reasoning "it is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative.").

132 *See* Ashdown, *supra* note 130, at 1315.

133 *White,* 401 U.S. at 782 (Harlan, J., dissenting).

134 *Id.* at 752.

135 Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1087 (2002).

136 *Id.*

137 *Riley*, 573 U.S. at 407–08 (Alito, J., concurring).

legislature which has the affordance of being proactive.[138] There lies little rationale in applying the outdated precedent of *Katz*, given that so little is private in the digital age. The void that the obsolete *Katz* left must be filled legislatively to help deem what data can be considered private.[139]

1. Why the ECPA Holds the Key

Since its conception in 1986, the ECPA has been amended numerous times.[140] However, none of the amendments adequately protected the electronic information of private citizens to the extent necessary in today's digital age.[141] The ECPA has not yet been amended to adapt to the technology of today to provide adequate Fourth Amendment protections. The ECPA holds the key because unlike the Fourth Amendment, which regulates only the government and private parties acting on the government's behalf, the ECPA recognizes that private parties acting on their own can pose a serious danger to digital privacy.[142]

While Congress may not have considered the technology-driven society we live in today when the ECPA was written, it is nonetheless the body that should address society's advances in technology.[143] Several jurisdictions have already considered the ECPA's shortcomings in this respect; several states have enacted legislation affording stronger protection to digital information than the federal ECPA.[144] This action by the states shows not only that the legislature is capable of adequately enforcing these protections but that, presently, the ECPA has failed to do so thus far. Although the amendments made to the ECPA thus far have failed to adapt to the digital age, they are nevertheless the perfect conduit for doing so.[145]

---

138 Charles E. MacLean, *Katz on a Hot Tin Roof: The Reasonable Expectation of Privacy Doctrine is Rudderless in the Digital Age, Unless Congress Continually Resets the Privacy Bar*, 24 ALB. L.J. SCI. & TECH. 47, 67 (2014).

139 *Id.* at 68.

140 Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 871 (2004).

141 *Id.*

142 *Id.* at 872 (explaining as an example that ". . . if America Online can look through the e-mails of its 30 million subscribers and disclose the evidence to the police without restriction, this would gut Internet privacy protections. The Fourth Amendment does not restrict this disclosure, but ECPA does: in addition to restricting the ability of law enforcement to order private ISPs [internet service providers] to disclose communications to law enforcement, the law also restricts the ability of private ISPs to disclose communications to law enforcement voluntarily.").

143 *See* discussion *supra* Part III(D)(i). Unlike the Fourth Amendment, which regulates only the government and private parties acting on the government's behalf, the ECPA also regulates private parties acting on their own.

144 Kim Zetter, *California Now Has the Nation's Best Digital Privacy Law*, WIRED (Oct. 8, 2015), https://www.wired.com/2015/10/california-now-nations-best-digital-privacy-law/.

145 *See, e.g., id.*

Courts have generally deferred to Congress on ECPA issues.[146] However, because Congress has not reformed the ECPA to provide guidance with respect to the technological boom, courts have inconsistently applied the statute.[147] Today's technology requires a new analysis because of how expansive and different technology is compared to when the ECPA was enacted; modern technology is fraught with exponentially more data.[148] The courts' inconsistent analyses show that the judiciary defers in whole to Congress on digital privacy issues. Moreover, the previously examined cases show that judges all the way up to the Supreme Court lack the ability to aptly apply and understand technological differences. Judges are, however, acutely aware of this issue.[149] Additionally, the government has expressed similar concerns and promoted a legislation-based solution to this issue.[150] Many factors and considerations are at play with such a complex statutory change, and the courts do not have the expertise or time to do so. The legislature is equipped to promote this change and probe the complex relationship between the Fourth Amendment and technology.[151] The courts cannot, and should not, be left to decipher this statute which is inept to provide suitable guidance. For courts to provide consistent decisions on Fourth Amendment issues involving digital data, the legislature must act to recognize modern technology's implicit differences from the technologies that existed at the time of the ECPA's inception.

2. A Potential Mosaic Theory Framework Fix

The mosaic theory presents challenges to modern day Fourth Amendment jurisprudence (the *Katz* test), however, the *Katz* test is exceptionally outdated. For this reason, it makes sense that *Katz* should be done away with regards to digital content and new legislation should take its

146 Achal Oza, *Amend the ECPA: Fourth Amendment Protection Erodes as E-mails Get Dusty*, 88 B.U. L. REV. 1043, 1054–55 (2008).

147 *See* Meera Unnithan Sossamon, *Subpoenas and Social Networks: Fixing the Stored Communications Act in a Civil Litigation Context*, 57 LOY. L. REV. 619, 644 (2011).

148 *See* Peter Van Buren, *4 Ways the Fourth Amendment Won't Protect You Anymore*, MOTHERJONES (Jun. 26, 2014), http://www.motherjones.com/politics/2014/06/how-fourth-amendment-not-protect/.

149 *Riley*, 573 U.S. at 407–08 (Alito, J., concurring) (expressing a lack of confidence in the Court being the best entity to decipher the relationship between today's technology and the Fourth Amendment) (stating that "I would reconsider the question presented here if either Congress or state legislatures . . . enact legislation . . . .").

150 Brief of Amicus Curiae Michael Varco in Support of Respondent, Carpenter v. United States, 138 S. Ct. 293 (2017) (No. 16-402), at 29 (quoting *Jones*, 565 U.S. at 427–28 (Alito, J., concurring) (stating "[i]n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative" because a "legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way.")).

151 *See* U.S. CONST. Art. I, § 7.

place. The mosaic theory may challenge the *Katz* test, but nevertheless, it is a new, mosaic theory-esque legislation that should be enacted in place of *Katz*.

The mosaic theory gives rise to several challenges. The first is the fact that the mosaic theory is a highly subjective concept. Courts can choose whether to apply it, and the premises for doing so are extraordinarily varied. The mosaic theory is not a concrete legal concept, but rather a theory upon which many courts have begun to rely.[152] As such, the mosaic theory brings with it many questions that the courts must address.

The first of these questions is that of a standard. This is necessary if courts are to adopt the mosaic theory. This is important when observing mosaic theory interpretations of the past; one need only look to the pro-mosaic opinions of *Maynard* and *Jones* to see that the same case can be interpreted many different ways.[153]

Although the three examples that will be mentioned analyze the *Maynard* and *Jones* cases differently, they all agree on one thing: it is the collective sum of government action, not the individual steps, which must be analyzed to determine what counts as a Fourth Amendment search.[154]

As previously discussed, the D.C. Circuit's viewpoint in *Maynard* asked whether the government learned more than a stranger could have observed.[155] This opinion introduced the mosaic theory.[156] The court viewed government conduct as violating one's reasonable expectation of privacy depending on the likelihood that the evidence collected was exposed to the public.[157] However, this claim was one that blanketed the entirety of the GPS monitoring—the whole twenty-eight days the respondent was surveilled—not just the individual pieces.[158] In the Circuit Court's opinion, the monitoring in the *Maynard* and *Jones* amounted to a search because it was highly unlikely that the public would observe the entirety of the respondent's actions.[159] The public could, indeed, have witnessed individual parts of Jones' movements, but it was essentially improbable for an individual to observe the entirety.[160] The court wrote that the collective sum of the twenty-eight days of surveillance revealed more than the sum of its parts; the non-

---

152 David E. Pozen, *The Mosaic Theory, National Security, and the Freedom of Information Act*, 115 YALE L.J. 628, 631 (2005).

153 *See Maynard*, 615 F.3d at 562; *see also Jones*, 565 U.S. at 400–13.

154 *See Maynard*, 615 F.3d at 561–62; *see also Jones*, 565 U.S. at 416 (Sotomayor, J., concurring).

155 *Maynard*, 615 F.3d at 560.

156 *Id.* at 562.

157 *Id*. at 558–59.

158 *Id.* at 560–61.

159 *Id.*; *see also Jones*, 565 U.S. at 416 (Sotomayor, J., concurring).

160 *See Maynard*, 615 F.3d at 560–61.

searches taken in aggregate became a search because while the individual pieces seem meaningless in isolation, when assembled together they painted a mosaic revealing a clear picture of one's life.[161]

Justice Alito's interpretation in the *Jones* case looked at societal expectations with regard to the practices of law enforcement.[162] From his point of view, a search occurs when investigators amass and analyze evidence in a fashion which would concern members of society.[163] In his concurrence, Justice Alito analyzed the case by asking whether the respondent's reasonable expectations of privacy were violated by long term monitoring of his vehicle.[164] Alito then went on to make the claim that this monitoring encroaches on expectations of privacy.[165] This type of monitoring would concern members of society because it is expected that law enforcement agents would not, but also that they could not, secretly monitor and index every movement of one's car for such a long period of time.[166]

Conversely, Justice Sotomayor looked at government power in her *Jones* concurrence.[167] If the government can learn details about an individual's personal life more or less at will, a search has occurred.[168] In her concurrence, she argued that when assessing objective reasonableness per *Katz*, it is pertinent the monitoring paint a detailed, comprehensive record of one's public movements that reflects a wealth of detail about a person's family, political views, profession, religion, and other associations.[169] Justice Sotomayor took the stance that even the most seemingly innocuous data might be relevant to constitutional protection.[170]

Another question pertaining to the mosaic theory that needs to be addressed is when the mosaic begins. In traditional Fourth Amendment application, generally only the question of how the information is acquired is of particular interest. However, now that the mosaic theory has entered the arena, the question becomes where the mosaic begins in terms of surveillance.[171] As the mosaic theory articulates that it is the taking together of data to create a clear picture of an individual, it evidently extends beyond the acquisition of information stage, which is typically where traditional

161 *Maynard*, 615 F.3d at 562.
162 *Jones*, 565 U.S. at 430 (Alito, J., concurring).
163 *Id.*
164 *Id.*
165 *Id.*
166 *Id.*
167 *Id.* at 416 (Sotomayor, J., concurring).
168 *Jones*, 565 U.S. at 414 (Sotomayor, J., concurring).
169 *Id.* at 415-16.
170 *See id.*
171 *See, e.g.,* Dennis, *supra* note 59, at 768.

Fourth Amendment application stops.[172] Aggregating the data that builds the mosaic requires taking it a step further—analyzing the data.

Moreover, the question of how much data is enough to make a viable mosaic must be answered. The GPS device in *United States v. Jones* was installed for twenty-eight days, which was deemed by Justice Alito as "definitely" being long enough; however, he presented no reasoning as to why this was the case.[173] Where is the line drawn? Was it drawn at two days—or at twenty-eight? This is a critical question.[174]

The general focus when it comes to the mosaic theory has been GPS surveillance, however, mosaics can be pieced together with other sorts of data as well. Taking one's web searches/sites visited, telephone numbers called, and emails in aggregate paints a clear picture of one's life even without location monitoring. Does the mosaic theory apply here as well? Add location data, and an even clearer profile of the surveilled individual can be put together. While the mosaic theory may present challenges to the *Katz* test used to analyze Fourth Amendment claims, the philosophy underlying it is precisely what would make for a revitalized approach to these claims in the digital age.

## IV. CONCLUSION

The courts have presented few, if any, alternatives to *Katz*; however, it is evident that there is work that needs to be done in securing privacy rights in the digital age. While today's technology has innumerable benefits, it can also be used to gather information about individuals that would otherwise require a warrant. Cell phones are an omnipresent aspect of the modern age and with their capabilities, they are able to paint a startlingly clear picture of one's life. Adding to this is the third-party doctrine, which essentially declares that there is no legitimate expectation of privacy in information that has been voluntarily turned over to third parties.[175] This would include information obtained by an individual's cell phone provider.[176] Public actions, such as traveling in a car, are likewise not afforded a reasonable expectation of privacy.[177] By this logic, then, there is not much in this digital age entitled to a "reasonable expectation of privacy" as posited by *Katz*.[178]

---

172 *See, e.g., id.*

173 *Jones*, 565 U.S. at 430 (Alito, J., concurring).

174 *See* Kerr, *supra* note 61, at 333–34. Kerr's article analyzes the length of time needed to create a viable mosaic and demonstrates that this is a critical, yet extremely complicated question. Courts must make fact-specific determinations of how much data is enough to make a viable mosaic.

175 *See, e.g., Smith*, 442 U.S. at 743–44.

176 *Id.* at 742–43.

177 *See, e.g., Knotts*, 460 U.S. at 281.

178 *See Katz*, 389 U.S. at 362.

This suggests that the capabilities of today's technologies should be shaping the average individual's perception of their privacy; the problem with this is that, barring the "tech-savvy," many individuals are unaware of the intricate capabilities of their devices or, perhaps more importantly, the doctrine that underlies it. This presents a challenge to the Fourth Amendment of the Constitution.

The technological developments of today have placed a tremendous amount of stress on the frameworks for Fourth Amendment privacy protections. These frameworks developed in an era when electronics did not exist or otherwise were not prevalent, and the Supreme Court has been unsuccessful in keeping up with the application of the Fourth Amendment with today's technology. For courts to provide consistent decisions on Fourth Amendment issues involving digital data, the legislature must act to recognize modern technology's implicit differences from the technologies that existed at the time of the ECPA's inception.