Living in Private: The Fourth Amendment and Perpetual Electronic Surveillance

Simon August Poser*

TABLE OF CONTENTS

* J.D., May 2024, The George Washington University Law School. Associate, Federal Communications Law Journal, Volume 76. B.A., 2019, Political Science, Haverford College. I would like to thank the Volume 76 FCLJ Editorial Board as well as Professors Ethan Lucarelli and Renée Lettow Lerner for their guidance during the publication process. I would also like to thank my incredible family for their endless support and love.

I. INTRODUCTION

The perennial debate over the balance between public safety and personal privacy presents vexing questions about the scope of governmental authority. Should the government be able to watch a person in public forever even if there is no reason to think they are doing anything illegal? What if they decide to monitor the outside of someone's home for months on end, around the clock, hoping to catch them doing something suspicious that will allow officers to apprehend them or search their home?[1]

A central legal question in the 21st Century has been how to understand the Fourth Amendment's protections in the context of the digital age. The Supreme Court and the lower federal courts have frequently grappled with how to apply the Fourth Amendment to modern surveillance technologies, which have given the government capabilities far beyond anything the founding generation could have imagined.[2][3] Such technologies include drones,[4] stationary pole cameras,[5] and artificial intelligence systems that aggregate data collected from street cameras and license plate readers.[6]

The Supreme Court has said that one of the Fourth Amendment's goals is "to place obstacles in the way" of police surveillance that is overly pervasive.[7] Despite this sentiment, the Court has been reticent to create clear rules and standards to govern uses of advanced surveillance technologies.

It is time for the Supreme Court to develop a new test to define when surveillance becomes too widespread, detailed, and targeted such that even limiting deployment to public areas encroaches on an individual's right to privacy. The proposed test would be two-pronged. The first prong of the test should be based around factors the Supreme Court has articulated in previous Fourth Amendment cases where the technology: (1) creates a historic record of information that can be stored and perpetually utilized; (2) gives government agents the ability to monitor persons or areas with superhuman precision; and (3) is prolonged and complete to the point where they are constructively treating the person as the target of a criminal investigation. If law enforcement seeks to use technology that meets the factors of this test, then at minimum a warrant supported by probable cause should be required. The second prong of the test would be that if one of the factors above is lacking, but the technique at issue is so extreme in some respect that it intrudes upon an individual's expectation of privacy in the totality of their movements, then it would similarly require a warrant supported by probable cause.

---

1. *See generally* United States v. Moore-Bush, 36 F.4th 320 (1st Cir. 2022).
2. *See* U.S. CONST. amend. IV.
3. *See generally* Riley v. California, 573 U.S. 373 (2014) (ruling that the search incident to arrest of a cellphone was unlawful under the Fourth Amendment).
4. *See generally* Brief for Center on Privacy & Technology at Georgetown Law as Amicus Curiae Supporting Appellant's Petition for Rehearing *En Banc*, Leaders of a Beautiful Struggle, et. al., v. Balt. Police Dep't, 979 F.3d 219 (4th Cir. 2020) (No. 20-1495), 2020 WL 7024181.
5. *See generally Moore-Bush*, 36 F.4th at 320.
6. *See* United States v. Lambert, No. 21-CR-00585 (VEC), 2022 WL 2873225, at *1 (S.D.N.Y. July 21, 2022).
7. *See* United States v. Di Re, 332 U.S. 581, 595 (1948).

This Note examines a current gap in the Supreme Court's Fourth Amendment jurisprudence, which deals with the use of these technologies to track individuals in public areas. Section II will discuss the history of Fourth Amendment jurisprudence, how it has been applied to electronic surveillance, and the live legal issues that form the basis of this Note's analysis. First, in Section II-A the Note will discuss some of the modern technologies that have complicated existing privacy law jurisprudence. Next, Section II-B will delineate the governing test used to determine when government actions violate a person's right to privacy. Section II-C through II-E will discuss the Supreme Court's applications of this test to forms of electronic surveillance. Finally, Section II-F will explore the most recent lower court decisions and the conflicting nature of their rulings pertaining to the lawfulness of various forms of electronic surveillance. Section III will restate the problem presented by advanced forms of surveillance and explain the two-prong test this Note proposes for courts to use in evaluating governmental surveillance techniques. Section IV will restate the conclusions of this Note, highlighting the need for a new privacy test for modern surveillance technologies.

II. BACKGROUND

A. The Evolution of Surveillance Techniques

Surveillance techniques, as they have advanced, can generally be described as improving two modes of surveillance capability: (1) how much information can be obtained about a target and (2) how many targets can be monitored at once.[8] Surveillance techniques are obviously not developed by legal professionals, and often Fourth Amendment doctrine can be slow to adapt to technological advances utilized by law enforcement.[9]

While there are too many technologies to list individually in this section, the surveillance technologies that have received the most attention from courts, and those with which this Note is concerned, are best described as "enhanced audio-visual surveillance" or "persistent video surveillance." These terms collectively refer to technologies that allow law enforcement to observe persons, hear communications, and monitor locations that they would

8. *See generally* Anne T. McKenna & Clifford S. Fishman, *Wiretapping and Eavesdropping: Surveillance in the Internet Age* § 30:1 (3d ed. 2007) ("Historically, it has made sense to address 'enhanced visual' surveillance and 'other forms of surveillance technology' through focus on specific forms of visual surveillance technology such as artificial illumination, aerial surveillance, image magnification, video surveillance, unmanned aerial vehicles or drones, satellites, and so on."); *see also* Anthony P. Picadio, *Privacy in the Age of Surveillance: Technological Surveillance and the Fourth Amendment,* 90 PA. B.A. Q. 162, 176-79 (2019) (describing forms of surveillance and their application in modern law enforcement entities).

9. *See* McKenna & Fishman, *supra* note 8, § 30.2 (noting that "[t]oday's cyber era . . . poses increasingly complex legal questions that do not fit easily within the Supreme Court's existing Fourth Amendment jurisprudence").

ordinarily not be able to, either because of limited human capabilities or limited law enforcement resources generally.[10]

Another key development in surveillance technology is the ability of security systems to efficiently aggregate and filter data from multiple sources, in order to identify patterns of behavior and alert police to potential investigative targets, such as the many street cameras that populate urban areas or automatic license plate readers.[11] This use of automated systems to uncover suspicious behaviors has been analyzed as a potential Fourth Amendment violation in and of itself.[12] For the purposes of this Note, it is simply relevant in illustrating that the aggregation of surveillance data presents and will continue to cause significant concerns as data collection systems improve in capacity and become more widely distributed.[13]

"Big Data"[14] analytics and Artificial Intelligence (AI)[15] systems, which analyze the information gathered by these tools, have been shown to have concerning applications with respect to social media platforms and law enforcement.[16] Two examples exemplify these emerging issues. The first is a cyber-surveillance tool called Geofeedia, which is an A.I. platform service that uses analytics to track social media posts by location; the tool does this through "a process known as 'geofencing' to draw a virtual barrier around a particular geographic region," and is able to collect and analyze public social media posts within that demarcated area.[17] This tool has been used by law

10. *See id.* (describing forms of surveillance such as "aerial surveillance (planes, UAVs, and satellites) . . . pole cameras, [and] video surveillance of private locations"); *see also* Christopher Slobogin*, Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 216 (2002).

11. *See* Mariana Oliver & Matthew B. Kugler, *Surveying Surveillance: A National Study of Police Department Surveillance Technologies*, 54 ARIZ. ST. L.J. 103, 104 (2022) (describing use of "aggregation of automated license-plate-reader data" to identify rioter from the January 6th insurrection).

12. *See generally* Elizabeth E. Joh, *The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing*, 10 HARV. L. & POL'Y REV. 15 (2016).

13. *See generally* Chris Gelardi, *Inside D.C. Police's Sprawling Network Of Surveillance*, THE INTERCEPT (Jun. 18 2022 6:44 AM), https://theintercept.com/2022/06/18/dc-police-surveillance-network-protests/ [https://perma.cc/H9NG-4U6H].

14. While "Big Data" can be a nebulous term, a good definition is that it "is a generalized, imprecise term that refers to the use of large data sets in data science and predictive analytics." Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93, 96 (2014).

15. *See generally What is artificial intelligence (AI)?*, IBM, https://www.ibm.com/topics/artificial-intelligence [https://perma.cc/ZWM2-CWR5] (last visited March 28, 2023).

16. *See* Margaret Hu, *Big Data Blacklisting*, 67 FLA. L. REV. 1735, 1773-76 (2015) (discussing various applications of data analytics programs by law enforcement).

17. Margaret Hu, *Cybersurveillance Intrusions and an Evolving Katz Privacy Test*, 55 AM. CRIM. L. REV. 127, 128-29 (2018). Geofeedia did this by aggregating data from the top social media sites (Facebook, Twitter, Instagram, etc.), identifying individuals who had posted within an area during a selected timeframe.

enforcement, and has sustained public scrutiny and criticism for its use in monitoring domestic protests in the United States.[18]

The second example of a collaboration tool between data analytics technology and law enforcement is "Future Attribute Screening Technology" (FAST). FAST, which has primarily been developed by the Department of Homeland Security (DHS), is another data analytics tool that filters "physiological and behavioral signals with the goal of identifying 'malintent': an individual's predilection for disruptive or violent behavior."[19] FAST was developed post-9/11 to aid law enforcement in identifying security threats by utilizing complex algorithms to identify vital signs (heart rate, eye movements, respiratory quality, etc.) associated with bad intent, deception, and malice.[20] These technologies have not been litigated to any significant extent by the courts, but even if they were, for reasons discussed below, they would likely not be regulated by current Fourth Amendment doctrine. *See infra* § III.A.

A final area that is worthy of note is facial recognition technology. Facial recognition technology allows law enforcement to compile facial images from driver's license records, previous bookings, and social media accounts, and then use computer algorithms to effortlessly compare them to monitor and identify individuals in real time.[21] While it may surprise some readers, facial recognition has existed since the beginning of this century and was first deployed by law enforcement agents in England.[22] As of the writing of this Note there has been no prominent case law discussing the legality of these systems in the criminal context, and action pushing back against them has largely been either through legislation or civil suits.[23] Given the potential for abuse that this catalog of personal information could pose, it is likely to be the subject of litigation in the near future.

B. The Fourth Amendment's Protections

The Fourth Amendment to the United States Constitution provides that searches and seizures by the government generally require a warrant supported by probable cause.[24] If a governmental action is considered a search, it requires a showing of probable cause by law enforcement that a

---

18. *See generally* Jonah Engel Bromwich, Daniel Victor & Mike Isaac, *Police Use Surveillance Tool to Scan Social Media, A.C.L.U. Says*, N.Y. TIMES (Oct. 11, 2016), https://www.nytimes.com/2016/10/12/technology/aclu-facebook-twitter-instagram-geofeedia.html?_r=0 [https://perma.cc/M8M8-S85S].

19. *See* Hu, *supra* note 16, at 129.

20. *See id.* at 136; *see also Privacy Impact Assessment For The Future Attribute Screening Technology (Fast) Project,* U.S. DEP'T OF HOMELAND SEC., at 2 (Dec. 15, 2008), https://www.dhs.gov/sites/default/files/publications/privacy_pia_012-s%26t_fast-2008.pdf [https://perma.cc/2SSS-CEAP?type=image].

21. *See* Harvey Gee, *Surveillance State: Fourth Amendment Law, Big Data Policing, and Facial Recognition Technology*, 21 BERKELEY J. AFR.-AM. L. & POL'Y 43, 76-78 (2021).

22. *See* Christopher Benjamin, *Shot Spotter and Faceit: The Tools of Mass Monitoring*, 6 UCLA J.L. & TECH. 2 (2002).

23. *See, e.g.*, Gee, *supra* note 21, at 78-82.

24. *See* U.S. CONST. amend. IV.

crime has been or will be committed and that the search is needed to uncover evidence of that crime.[25] Otherwise the governmental action is unconstitutional and evidence gathered from the unlawful search is generally suppressed.[26] This is the central policy question underlying the debate over the reach of the Fourth Amendment: what government actions are so intrusive to a person's privacy that they require a showing of probable cause to support them?

Until the mid-twentieth century, the Fourth Amendment primarily protected private property against physical trespasses and seizures of a person's effects.[27] The came *Katz v. United States*, where the Supreme Court made a significant shift in Fourth Amendment jurisprudence by holding that it did not simply protect people's property from trespass by government agents, but also protected their personal privacy even when no physical trespass occurred.[28] In his concurrence, Justice Harlan outlined a two-pronged test for determining when the government's actions should be considered a "search" under the Fourth Amendment.[29] Harlan wrote that the fundamental questions for applying Fourth Amendment protection are whether an individual first "exhibited an actual (subjective) expectation of privacy [in a place or thing] and, second, that the expectation be one that society is prepared to recognize as reasonable."[30] Harlan's test, which has come to be known as the "Katz Test" or the "Reasonable Expectation of Privacy Test," has been the dominant method used to determine whether a search has occurred under the Fourth Amendment, and is invariably invoked in cases that involve electronic surveillance.[31]

Katz remains the dominant test in the general body of Fourth Amendment jurisprudence, but it has invariably sustained criticism in its long

---

25. While it is not relevant to the subject matter of this note, it bears mention that a multitude of exceptions to the warrant requirement have been created by the Supreme Court over time. *See, e.g.*, Carroll v. United States, 267 U.S. 132, 153 (1925) (creating the automobile exception); Nix v. Williams, 467 U.S. 431 (1984) (establishing the inevitable discovery exception for evidence collected from a warrantless search); Brigham City v. Stuart, 547 U.S. 398, 402 (2006) (applying the exigent circumstances exception to justify warrantless entry of a home).

26. *See* United States v. Bershchansky, 788 F.3d 102, 112 (2d Cir. 2015) ("To safeguard Fourth Amendment rights, the Supreme Court created 'an exclusionary rule that, when applicable, forbids the use of improperly obtained evidence at trial.'") (quoting Herring v. United States, 555 U.S. 135, 139 (2009)).

27. *See* Orin S. Kerr, *Katz as Originalism*, 71 DUKE L.J. 1047, 1079 (2022).

28. *See* Katz v. United States, 389 U.S. 347, 353 (1967) (holding that the government's warrantless eavesdropping of the defendant's conversation inside a phone booth constituted a search because he had manifested a subjective expectation of privacy in the conversation he was having in the phone booth).

29. *Id.*

30. *See id.* (internal marks omitted).

31. *See, e.g.*, Margaret Hu, *Cybersurveillance Intrusions and an Evolving Katz Privacy Test*, 55 AM. CRIM. L. REV. 127, pincite (2018) ("For 50 years, *Katz v. United States* has defined the federal courts' approach to evaluating what is a 'reasonable' law enforcement action under the Fourth Amendment."); Florida v. Jardines, 569 U.S. 1, 12 (2013) (Kagan, J., concurring) (noting that while the majority resolved the case under the physical trespass rule, the *Katz* expectations of privacy test could also apply to reach the same result).

history of use.[32] One of the reasons is that defining an expectation of privacy is difficult given the endless variety of factual scenarios for the court to consider.[33] The *Katz* test was based on the idea that where it is reasonable for citizens to *expect* privacy, the Fourth Amendment should protect that privacy.[34] A person sitting inside their home should expect no one is watching them, and therefore, the government may not take steps to observe that individual within their home unless there is probable cause to believe that doing so will uncover a crime.

C. The Supreme Court's Electronic Surveillance Cases

Two Supreme Court cases considering the legality of electronic surveillance prior to *Carpenter* are critical to understanding the difficult questions underlying modern Fourth Amendment jurisprudence. The first of these cases is *United States* v. *Knotts.*[35] In *Knotts*, the Court held that the government's clandestine placement of a radio transmitting beeper in a package the defendant subsequently put inside of his car was not a search.[36] The Court's holding was based in part on the fact that the beeper principally allowed the government to track the defendant on public roads, where there would be no expectation that a person's movements would be private.[37] The Court emphasized the minimal information the radio transmitter could provide and distinguished it from surveillance that could reveal more detailed varieties of information.[38]

The second key case in the Supreme Court's Fourth Amendment jurisprudence on electronic tracking came in *United States* v. *Jones*.[39] In *Jones*, the court confronted the question of whether the attachment of a GPS tracking device to a car is a search under the Fourth Amendment. The D.C. Circuit, which ruled on the case before the Supreme Court granted certiorari, distinguished *Knotts*, finding that the *totality* of Jones' movements was *not*

32. *See Kerr*, *supra* note 27 at 1048 ("Over fifty years later, the *Katz* expectation of privacy test has come under widespread attack. No one likes *Katz*, it seems. Everyone wants to replace it with something else, even if no one agrees on what its replacement should be.").

33. *Compare* Florida v. Riley, 488 U.S. 445, 448-50 (1989) (holding that aerial surveillance of the curtilage of a defendant's home by a helicopter hovering at 400 feet above the ground did violate any reasonable expectation of privacy) *with* Bond v. United States, 529 U.S. 334 (2000) (holding that police squeezing the exterior of a bag to detect drugs did violate the defendant's reasonable expectation of privacy in their belongings).

34. *See Bond*, 529 U.S. at 351 (explaining that "[T]he Fourth Amendment protects people, not places. What a person *knowingly exposes* to the public, even in his own home or office, is not a subject of Fourth Amendment protection.") (emphasis added).

35. United States v. Knotts, 460 U.S. 276 (1983).

36. *See id.* at 285.

37. *See id.* at 281 (holding that a "person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another").

38. *See id.* at 284 (noting the government made "limited use . . . of the signals from this particular beeper").

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

exposed to the public, and thus merited protection under the *Katz* "reasonable expectations of privacy" test.

> [T]he totality of Jones's movements over the course of a month—was not exposed to the public: First, unlike one's movements during a single journey, the whole of one's movements over the course of a month is not actually exposed to the public because the likelihood anyone will observe all those movements is effectively nil. Second, the whole of one's movements is not exposed constructively even though each individual movement is exposed, because that whole reveals more—sometimes a great deal more—than does the sum of its parts . . . Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble . . . Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month. The sequence of a person's movements can reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story. A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts.[40]

The D.C. Circuit opinion in *Maynard* reflected a nuanced view of the *Katz* test, that the government may not make a "divide and conquer" Fourth Amendment argument by suggesting all its actions taken individually were not a search, so their use of the tracker was lawful; rather, the question the D.C. Circuit asked was whether, taken together, the actions taken by the government harmed a reasonable privacy interest of the defendant.[41] The case was then appealed to the Supreme Court, which took a different route to reach the same result.

In *Jones*, the Supreme Court avoided settling many of these difficult questions. Instead, it simply ruled it was a search to attach a tracker to the defendant's car because that required trespassing on his effects.[42] However, in the concurrences to the opinion five justices espoused or supported some variant of the view that warrantless GPS tracking of a vehicle, even if done without physical trespass upon the vehicle itself, could be considered a search

40. *See* United States v. Maynard, 615 F.3d 544, 558-62 (D.C. Cir. 2010), *aff'd in part sub nom Jones*, 565 U.S. 400 (cleaned up).

41. *Maynard*, 615 F.3d at 561.

42. *See Jones*, 564 U.S. at 404.

under the *Katz* "reasonable expectation of privacy" test.[43] The majority did note that many "thorny problems" could lie ahead with respect to expectations of privacy in electronic records, but decided to resolve the case on a more narrow ground by using the trespass rule.[44] The decision of *Jones* was unanimous, but the concurrences reflected a diverse array of perspectives as to how to think about an individual's privacy in the totality of their movements, and set the stage for further cases wrestling with how to apply the Fourth Amendment to electronic surveillance methods.[45]

D. Permutations of Katz*: The Mosaic Theory and Third-Party Doctrine*

Given the expansive nature of the *Katz* test, many "sub-doctrines" have been suggested for or created by courts to expound upon it; two such doctrines will be discussed here as they are useful in delineating the modern surveillance issues this Note attempts to address: The Third-Party Doctrine the Mosaic Theory.

The first outgrowth of the *Katz* test critical to understanding the caselaw regarding privacy is the Third-Party Doctrine. The Third-Party Doctrine generally holds that records of individuals which are held by third parties are not subject to the warrant requirement.[46] The Third-Party Doctrine was created by the Supreme Court to distinguish information that individuals solely possess and information that individuals give over to third parties (and, thus, over which they have reduced privacy rights). For example, in *Smith v. Maryland*, the Supreme Court held that a law enforcement officer's use of a pen register to record all the numbers dialed from a person's phone was not a search.[47] The Supreme Court, for about forty years, created few substantial limits on the Third-Party Doctrine, until they carved out one notable exception to it in 2018 discussed in the next subsection.

The second sub-doctrine that emerged as a gloss on the *Katz* test came after the Court decided *Jones* and is known as the "Mosaic Theory". The Mosaic Theory was introduced as a theory to explain the rationales behind the concurrences of the justices in *Jones* who were skeptical of warrantless long-term GPS monitoring, irrespective of the placement of the tracker on the car.[48] The exact origins of this theory are unclear, but it is most closely associated

43. *See generally id.* at 413-18 (Sotomayor, J., concurring); *id.* at 419-31 (Alito, J., concurring, joined by Ginsburg, Breyer, and Kagan, JJ.).

44. *See id.* at 412-13.

45. *See, e.g.*, *Jones*, 565 U.S. at 415-16 (Sotomayor, J., concurring) (noting that the Fourth Amendment may be implicated when police utilize "a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations").

46. *See* Smith v. Maryland*,* 442 U.S. 735, 743-44 (1979) (holding that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties").

47. *See id.*; *see also* United States v. Miller, 425 U.S. 435 (1976) (holding there was no reasonable expectation of privacy in financial records held by a bank).

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

with Professor Orin Kerr.[49] The Mosaic Theory's central claim is that courts can, and should, analyze a "collective sequence" of government actions to ascertain whether the Fourth Amendment has been violated.[50] The subsequent axiom of the Mosaic Theory is that if through prolonged surveillance law enforcement allows the government a kind of information about an individual that could only be gleaned from constant monitoring, that may implicate a person's Fourth Amendment interests.[51]

There are a few problems with the Mosaic Theory. First, the proposition it stands for is not particularly remarkable. Putting together individual pieces of information that, when combined, reveal an individual is engaged in a criminal enterprise, constitutes the essence of investigatory work; thus, an expansive view of the Mosaic Theory could render completely normal police practices unconstitutional.[52] Second, the Mosaic Theory does not explain how widely the scope of the analysis should sweep. That is, how many government actions need to be analyzed together, and are there any ways to distinguish one action from others conducted during the same period? Finally, the Mosaic Theory is devoid of any particularized or objective factors that can be effectively administered by courts. Therefore, it is not an established or sufficient alternative to the *Katz* test, or for the test this Note proposes for advanced surveillance technologies. However, it is important to note as a background principle for the proposition that government actions can and sometimes should be analyzed collectively rather than individually.

E. The Supreme Court's New Understanding in Carpenter

The most recent Supreme Court case that grappled with the issue of warrantless searches of electronically maintained records was similar to *Jones* in that it raised more questions than it answered. In 2018, the Supreme Court decided *Carpenter* v. *United States*, in which it held that Cell-Site Location Information (CSLI), was protected against warrantless searches by the government.[53] *Carpenter* represented a seismic shift in the Court's understanding of how to apply the protections of the Fourth Amendment in the digital age. The relevant facts were that the government, while investigating a series of thefts, obtained court orders under the Stored Communications Act for the CSLI of the suspect's cell phones.[54] The government argued that CSLI is not controlled or maintained by the user of

49. *See id.* at 313.
50. *See id.* at 320-21.
51. *See id.* at 326-27.
52. *See id.* at 328-29.
53. 585 U.S. 296, 316-17 (2018).
54. *See id.* at 296. CSLI refers to time-stamped records a cellphone generates when it connects to radio towers. A cellphone generates this information automatically, and the records can be used in many instances to track the movements of an individual. In *Carpenter*, the government obtained almost thirteen thousand data points cataloging the suspect's movements over one hundred and twenty-seven days.

the cellphone and is, therefore, a third-party record (held by the service provider) in which the user has no reasonable expectation of privacy.[55]

The Court described the ubiquitous nature and extent of information kept on cellphones and concluded that the warrantless collection of CSLI was a violation of the Fourth Amendment.[56] Chief Justice Roberts, writing for a five-justice majority, described the "detailed, encyclopedic, and effortlessly compiled" nature of CSLI data, which was key to their analysis that the government's use of this data was concerning.[57] The majority found the CSLI data was entitled Fourth Amendment protections, in part because it gives law enforcement the ability to track any individual who owns or even possesses a cellphone without the need to "know in advance whether they want to follow a particular individual."[58] The majority concluded with a flourish:

> We decline to grant the state unrestricted access to a wireless carrier's database of physical location information. In light of the *deeply revealing nature of CSLI*, its depth, breadth, and comprehensive reach, and the *inescapable and automatic nature of its collection*, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection. The Government's acquisition of the cell-site records here was a search under that Amendment.[59]

The decision was fractious and generated several separate dissents that raised many issues regarding the Supreme Court's Fourth Amendment jurisprudence and its applicability to the realm of electronic surveillance.[60] These issues will be discussed in depth in Section III.

F. Post-Carpenter *Lower Courts*

In the four years since *Carpenter* was decided, lower courts have generally limited the application of its reasoning to CSLI, declining to extend Fourth Amendment protection to other types of electronic data.[61] However, in that time a number of lower courts have wrestled with how to understand

55. *See id.* at 313-14 (describing the government's argument that "the third-party doctrine governs this case . . . [because CSLI should be categorized as] 'business records' created and maintained by the wireless carriers").

56. *See id.* at 300-02; *Cf. Riley*, 573 U.S. at 393-94 (noting the "quantitative and . . . qualitative" differences between cellphones and other items a person possesses).

57. *See Carpenter*, 585 U.S. at 312.

58. *See id*.

59. *Carpenter*, 585 U.S. at 320 (emphasis added).

60. Justice Gorsuch in a lengthy dissent called the *Katz* test a way for the Supreme Court "to protect privacy in some ethereal way dependent on judicial intuitions." *See id.* at 392 (Gorsuch, J., dissenting). Justice Gorsuch dissented from the reasoning, not the result, opting to propose a textualist view of the Fourth Amendment whereby CSLI could be protected as a bailment. *See* Kerr, *Katz as Originalism*, *supra*, note 27 at 1089-92.

61. *See, e.g.*, United States v. Brown, 627 F. Supp. 3d 206 (E.D.N.Y. 2022) (denying a motion to suppress vehicle GPS data, in part because the privacy interests at play in the case are not the same as they were in *Carpenter*).

Carpenter and whether to extend it to factual contexts outside of CSLI. These will be examined in turn, as each of them makes important points about how this case has been extended or limited.

1. Remote GPS Tracking of Vehicles: *United States v. Diggs*

In 2019, less than a year after *Carpenter* was decided, a federal district court in Illinois held it was a search under the Fourth Amendment to access the historical GPS data of a car the defendant did not own.[62] The court held specifically that under the *Katz* test framework, the defendant had a reasonable expectation of privacy in his movements in the car, even though it was not an item he owned.[63] The court also explicitly invoked *Carpenter* to dismiss the government's argument that the third-party doctrine precluded the defendant from having standing to challenge the use of the data from his wife's car.[64] The government did suggest that the fact the GPS data captured the defendant's wife's movements as well as the defendant's reduced his privacy interest in it, but the district court considered that argument to be forfeited.[65] As of this writing, no circuit court has adopted the reasoning of *Diggs* to establish a rule that warrantless collection of GPS data from a car not owned by a defendant violates the Fourth Amendment. However, it has had some resonance outside the Seventh Circuit and prompted some courts to discuss its application.[66]

---

62. *See* United States v. Diggs, 385 F. Supp. 3d 648, 650-53 (N.D. Ill. 2019) (noting that the car at issue was registered to Diggs' wife and holding it was a violation of his rights to track with GPS data).

63. *See id.* at 651 ("[The defendant] had a reasonable expectation of privacy in his movements, as chronicled by a month's worth of GPS data tracking the vehicle he was driving.").

64. *See id.* at 653-54 (reasoning that "*Carpenter* defeats the government's third-party argument here . . . Applying the third-party doctrine to the GPS data here would require essentially the same extension of the doctrine that the [Supreme] Court rejected in *Carpenter* . . . Accordingly, *Carpenter* compels the conclusion that, given the privacy concerns implicated by the 'detailed and comprehensive record of [Diggs's] movements' captured by the Lexus's GPS tracker, 'the fact that the [police] obtained the information from a third party does not overcome [Diggs's] claim to Fourth Amendment protection.'") (internal citations omitted).

65. *See id.* at 652.

66. *See* United States v. Jackson, No. 2:21-CR-331-MHT-SMD, 2022 WL 1498191 (M.D. Ala. Mar. 15, 2022), *report and recommendation adopted,* No. 2:21CR331-MHT, 2022 WL 1491670, at *4-5 (M.D. Ala. May 11, 2022) (distinguishing *Diggs* in part by noting that the case at issue "presents a very different set of facts leading to a different result . . . The police did not aggregate historical GPS data to tell a detailed story about Jackson's movements over a period of time to link him to the rash of dollar store robberies [like in *Diggs*]. Rather, they used essentially real-time data to find a wanted car. This is a critical distinction that fundamentally distinguishes this case from Jones and Diggs."); *see also* United States v. Currie, No. 8:20-CR-00262-PWG, 2022 WL 195504, at *5-8 (D. Md. Jan. 21, 2022) (reasoning that like in *Diggs*, ownership of an item (in *Currie*, a cellphone) is not dispositive in determining whether an individual can assert a reasonable expectation of privacy over it).

2. Pole Cameras: *Tuggle*, *Moore-Bush*, and *Hay*

In 2021, the Seventh Circuit in *United States v. Tuggle* decided that law enforcement officers' use of stationary pole cameras on public utility poles was not a search under the Fourth Amendment.[67] Law enforcement, during the course of investigating a drug conspiracy, warrantlessly used three pole cameras to monitor the outside area of the defendant's house.[68] The court found the duration (eighteen months) concerning, but still declined to extend *Carpenter* to pole cameras.[69] This aspect of *Tuggle* shows how the *Katz* reasonable expectation of privacy test allows courts ways to let endless amounts of surveillance in places not guaranteed *per se* Fourth Amendment protection, such as the visible exterior of the home.[70]

In the Summer of 2022, the First Circuit considered whether prolonged surveillance of public areas was permissible.[71] In *United States v. Moore-Bush*, the First Circuit, sitting *en banc*, split evenly on the question of whether the government's use of a stationary pole camera, which was aimed at the front of the Defendant's house for over eight months, was a search under the Fourth Amendment.[72] That case demonstrates the continuing debate among the lower courts of how expansively to read the Supreme Court's ruling in *Carpenter* and whether they possess the institutional competence to adjudicate critical questions regarding personal privacy and the deployment of advanced digital surveillance technologies.

The Tenth Circuit considered a similar issue in *United States v. Hay*.[73] The opinion began by bluntly saying "[d]oes the Fourth Amendment permit the government to surveil a home for months on end without a warrant? This case requires us to decide."[74] *Hay* involved the investigation of a veteran's disability status; As part of their investigation, agents "installed a pole camera on a school rooftop across the street from Mr. Hay's house. The camera was remote-controlled and activated by motion, and it recorded near constant footage of Mr. Hay's house as visible from across the street. All told, the camera captured 15 hours of footage per day for 68 days."[75] Mr. Hay was

67. *See* United States v. Tuggle, 4 F.4th 505 (7th Cir. 2021), *cert. denied*, 142 S. Ct. 1107 (2022).

68. *See id.* at 511 ("The government installed three cameras on public property that viewed Tuggle's home. Agents mounted two cameras on a pole in an alley next to his residence and a third on a pole one block south of the other two cameras. The first two cameras viewed the front of Tuggle's home and an adjoining parking area. The third camera also viewed the outside of his home but primarily captured a shed owned by Tuggle's coconspirator and codefendant.").

69. *See id.* at 526-27.

70. *See id.* at 514 (Reasoning that surveilling the exterior of the defendant's home with pole cameras is not a search because "Tuggle knowingly exposed the areas captured by the three cameras. Namely, the outside of his house and his driveway were plainly visible to the public. He therefore did not have an expectation of privacy that society would be willing to accept as reasonable in what happened in front of his home.").

71. *See generally* United States v. Moore-Bush, 36 F.4th 320 (1st Cir. 2022).

72. *See Moore-Bush*, 36 F.4th at 321-60, 361-72.

73. 95 F.4th 1304 (10th Cir. 2024).

74. *Id.* at 1308.

75. *Id.*

convicted of ten counts of stealing government property in violation of 18 U.S.C. § 641 and six counts of wire fraud in violation of 18 U.S.C. § 1343.

Hay challenged the conviction in part on Fourth Amendment grounds, claiming that like the defendant in Carpenter, he had a reasonable expectation of privacy in the totality of his movements coming and going from his home. Hay argued on appeal that the government was able to "paint[] an intimate portrait of [his] personal life," including "when he entered and exited his home; who visited him and his family," and "what [he] did on his own front porch."[76] The 10th Circuit rejected this argument, noting that "No circuit court has concluded that extended video surveillance of a house is a search under *Carpenter*."[77] It did not matter that the length of monitoring was that long, or that the porch, which would be considered the curtilage of the home, was monitored. *Hay* represents the last word on this subject, and encapsulates the view of the lower federal courts that *Carpenter* is a narrow decision and its holding sweeps no more broadly than its facts.

3. Surveillance from the Sky: *LOABS v. Baltimore*

In 2021, the Fourth Circuit considered the constitutionality of an aerial surveillance program that was used by the Baltimore Police Department.[78] The program, known as the Aerial Investigation Research (AIR) program, was described by the Fourth Circuit as follows:

> The AIR program uses aerial photography to track movements related to serious crimes. Multiple planes fly distinct orbits above Baltimore, equipped with PSS's camera technology...The cameras capture roughly 32 square miles per image per second. The planes fly at least 40 hours a week, obtaining an estimated twelve hours of coverage of around 90% of the city each day, weather permitting. The PSA limits collection to daylight hours and limits the photographic resolution to one pixel per person or vehicle, though neither restriction is required by the technology. In other words, any single AIR image—captured once per second—includes around 32 square miles of Baltimore and can be magnified to a point where people and cars are individually visible, but only as blurred dots or blobs.[79]

76. *Id.* at 1316.

77. *See id*. (collecting authority); United States v. Dennis, 41 F.4th 732, 741 (5th Cir. 2022), *cert. denied*, 143 S. Ct. 2616 (2023) ("Surveillance of areas open to view of the public without any invasion of the property itself is not alone a violation.").

78. *See* Leaders for a Beautiful Struggle v. Balt. Police Dep't, 2 F.4th 330, 330-35 (4th Cir. 2021).

79. *See id.* at 334.

While it was only utilized during certain days of the week, the AIR program gave the police extraordinary surveillance powers.[80] Community advocates challenged the law, and were joined by an assortment of amici in arguing there were serious privacy concerns present with the warrantless use of this technology.[81] The Fourth Circuit, sitting *en banc*, concluded the case was moot based upon a series of factual developments, but a majority ruled that the use of the AIR program was a search, and its warrantless use violated the Fourth Amendment.[82]

4. Commonality of Issues and the Need for a New Standard

Like *Carpenter*, all of these lower court cases represent difficult situations because they expose how many extremely serious surveillance techniques can fall through the cracks of the Supreme Court's Fourth Amendment Jurisprudence. This Note does not argue that surveillance techniques of the kind described above may not be used, or even that they should all necessarily require a warrant. However, given the disparity of outcomes in these cases, the broader social milieu concerning privacy and the expansive reach of technology in modern life, there is a need for new legal rules to apply to disputes over governmental surveillance.

III. ANALYSIS

A. Problems Protecting Privacy

Looking at the current state of the law in its totality, existing Fourth Amendment doctrine has failed to adequately protect the privacy of individuals from many advanced forms of surveillance. The simple fact is that a vast amount of warrantless surveillance is currently occurring with minimal and unclear legal rules. The lower courts' attempts to apply existing caselaw to modern surveillance techniques have been at best uneven.[83] This Note does not call for a wholesale repeal of the *Katz* expectation of privacy test. As *Jones* shows, multiple legal standards can and should co-exist to safeguard core constitutional rights such as the Fourth Amendment.[84] Instead, this Note

80. *See* Scott A. Havener, *Leaders of A Beautiful Struggle v. Baltimore Police Department: The Fourth Amendment Continues Its Struggle to Make Sense of the Twenty-First Century*, 68 LOY. L. REV. 159, 163-64 (2021) ("During the daytime . . . three PSS aircraft would continuously circle Baltimore at altitudes between 3,000 and 12,000 feet. For no less than forty hours a week, each plane would take one photograph per second at a resolution of one pixel per 1.45 square feet, roughly representing a person as a single pixel. AIR was used to track vehicles' movements too, which were typically depicted as fifteen to twenty pixels. The combined imagery provided coverage of over ninety percent of the city.").

81. *See Leaders of a Beautiful Struggle*, 2 F.4th at 335.

82. *See* Havener, *supra*, note 75 at 163-67.

83. *See supra*, notes 67-78.

84. *See Jones*, 565 U.S. at 409 ("[T]he Katz reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test.") (emphasis in original).

argues that a new analytical framework should be developed to determine the reasonableness of modern surveillance techniques that currently pervade domestic law enforcement in the United States.

A new test is needed for three reasons. First, the *Katz* test's framework is unworkable in the context of modern surveillance tools. It is not reasonable to expect judges to consistently determine what the objective expectations of privacy amongst citizens are in regard to the types of activities discussed above, such as the totality of their movements as captured through GPS, the prolonged surveillance of their person or the exterior of their homes, or the measurement of their bodily signals or facial data.

Second, the *Katz* test is too susceptible to judicial interpretation and, as has been described, leads to inconsistent results.[85] The reason for this is that the *Katz* test is not an empirical test that answers the question of what the actual expectations of privacy are.[86] Rather, it is a normative test that judges use to answer the question of what societal expectations *should* be.[87] While this may be a formulation some would prefer, it gives enormous discretion to the judiciary without any accompanying doctrinal safeguards or limiting principles. Thus, there needs to be a test grounded in a set of relatively objective factors that, when met, should require the government to demonstrate probable cause.

Finally, the current regime is arguably too permissive towards mass surveillance techniques and contravenes the spirit of the Fourth Amendment by not protecting citizens from "permeating police surveillance."[88] There are a multitude of technologies in use today by the government that afford them immense surveillance capabilities and would likely go unchecked under current Fourth Amendment doctrine.[89] While a doctrinal test may come under some of the same criticisms leveled at the Mosaic Theory, it would standardize the case law in this area and allow courts more particularized criteria to assess surveillance techniques. At least one member of the current Supreme Court has put forth the somewhat out-of-the-box idea of treating electronic data generated by a person as a bailment (non-ownership transfer of possession) whereby they would retain ownership rights and associated privacy protections.[90] While this may come to pass in some form, that view garnered no support in *Carpenter*, and is unlikely to become ensconced in binding precedent on the lower courts anytime soon.

The Mosaic Theory, while useful to delineate the gap that permits long-term surveillance of individuals in public areas, is fairly unhelpful in providing courts an interpretive roadmap for those dissatisfied with *Katz* and

---

85. *See Carpenter*, 585 U.S. at 391 (Gorsuch, J., dissenting) (opining that the contours of the *Katz* "expectation of privacy test" are "left to the judicial imagination."); *see also* Hu, *supra* note 31.

86. *See Carpenter*, 585 U.S. at 391-95 (discussing ways of viewing the *Katz* test).

87. *See id.*

88. *See Di Re*, 332 U.S. at 595.

89. *See* Benjamin Goodman*, Shotspotter-the New Tool to Degrade What Is Left of the Fourth Amendment*, 54 UIC L. REV. 797, 824-28 (2021) (describing Seventh Circuit case in which the court found it reasonable for police to conduct a *Terry* stop based upon information they obtained from "Shotspotter," an automatic gunshot detection system).

90. *See Carpenter*, 585 U.S. at 396-405 (Gorsuch, J., dissenting).

its application to new technologies that "once seemed like science fiction."[91] Some recent scholarship has suggested the Supreme Court's *Carpenter* decision, adopting some tenets of the Mosaic Theory, has now provided a new set of questions for the lower courts, but that it largely restates the questions of the *Katz* test and does not add any new considerations to guide courts in assessing surveillance techniques.[92]

The question becomes how to move forward from our current landscape of porous Fourth Amendment law. There is a clear and present tension in the law that mandates the Supreme Court to provide some measure of clarity and consistency to the case law. When one examines the concurrences of *Jones*, the Court's opinion in *Carpenter*, and the post-*Carpenter* decisions, it becomes clear that there is widespread disagreement amongst courts and judges on how to handle the issue of warrantless surveillance.[93] *Carpenter* was anomalous in that the Supreme Court confronted a conflict in its own case law and chose to create a narrow exception to the third-party doctrine based on the unique nature of CSLI. The majority in *Carpenter* disclaimed any pretense that it provides a clear roadmap or test for the range of privacy issues presented by warrantless uses of other forms of technology.[94] It is far from certain that if the current Supreme Court justices confronted a case like *Carpenter,* the result would be the same, but in deference to the principle of *stare decisis* for the purpose of this Note it is assumed that the holding will remain.

The Supreme Court should act to remedy this gap in Fourth Amendment law, because they are the final arbiters of what the Constitution's protections mean.[95] Action from Congress, while it may be preferable to judicial rules given that Congress is democratically accountable, is unlikely to happen in this area given the complexity of these issues and the lack of appetite to impose regulations on the government's investigatory powers. Because of that, this Note argues for a test the Supreme Court should impose on the lower courts to assess Fourth Amendment interests for situations where the government uses advanced surveillance technology to either monitor people in public areas or conduct prolonged surveillance of a person without a warrant based upon probable cause. The Supreme Court should recognize

---

91. Taylor H. Wilson, Jr., *The Mosaic Theory's Two Steps: Surveying Carpenter in the Lower Courts*, 99 TEX. L. REV. ONLINE 155, 159 (2021) (quoting David Gray & Danielle Keats Citron, *A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy*, 14 N.C. J.L. & TECH. 381, 386 (2013)).

92. *See generally id*. (discussing the application of the *Katz* test to electronic surveillance technologies).

93. This statement is evident from a nothing more than a glance at the fractured votes behind the cases discussed in this Note. While the result of *Jones* was unanimous, multiple concurrences were generated that diverged from the majority's rationale significantly; the Supreme Court's decision in *Carpenter* was 5-4; the Seventh Circuit was divided in *Tuggle*; the Fourth Circuit *en banc* was divided in *Leaders of a Beautiful Struggle*; the First Circuit, in poetic fashion, evenly split down the middle in *Moore-Bush*, with three judges writing the government's actions constituted a search under the Fourth Amendment, and three writing they did not.

94. *See Carpenter*, 585 U.S. at 298.

95. *See, e.g.*, Cooper v. Aaron, 358 U.S. 1, 18 (1958) (explaining that "the federal judiciary is supreme in the exposition of the law of the Constitution").

that "[t]here comes a point where we should not be ignorant as judges of what we know to be true as citizens."[96] This Note submits that point has been reached, and that the *status quo* is not acceptable.

B. A New Test for a New Era

This Note proposes a two-prong test. The first prong involves an analysis based on the following three questions. Each of these inquiries is formulated to be as objectively determinable as possible and has been used in some form or fashion by the Court in its prior electronic surveillance cases. First, do the surveillance techniques of the government reveal information in real time, or does it also store and "mine" information about a person that predated the government's investigation? Second, do the techniques give the government superhuman capabilities to surveil an individual or multiple individuals with precision far beyond what could be achieved through human capabilities like stakeouts and other "real-time" surveillance? Finally, is the length of the monitoring by the surveillance technique such that it should not be reasonably used against a person unless there is probable cause to believe there was a crime? If any one of the elements above is not satisfied, then the court would move to the second prong of the test. The second prong is whether the surveillance at issue is so extreme and gathers information of such a sensitive nature that it has in effect intruded on an individual's expectation of privacy in the totality of their movements, and therefore, cannot be allowed without a warrant.

1. Retrospective v. Prospective Nature of the Information Collected

The first element of the proposed test asks an easily verifiable question: do the surveillance techniques employed by the government allow them to retrieve information about a person's movements from a time before the investigation of that individual began? If so, then the action merits intense scrutiny, as this gives law enforcement the option to "travel back in time" to chronicle the activities of any person they would like to investigate.[97] If the techniques are being used in real-time and are solely for the purpose of monitoring individuals already identified as suspects, then this element would not be implicated, and those methods could be analyzed under the traditional *Katz* framework to determine whether they require a warrant.

This element has informed the Supreme Court's analysis in prior cases dealing with electronic surveillance techniques.[98] In *Jones*, for example, the

96. *Cf.* United States v. Zubaydah, 142 S. Ct. 959, 985 (2022) (Gorsuch, J., dissenting).

97. *See Carpenter*, 598 U.S. at 311 ("Moreover, the *retrospective quality* of the data here gives police access to a category of information otherwise unknowable . . . With access to CSLI, the Government can now travel back in time to retrace a person's whereabouts.") (emphasis added).

98. *See Jones*, 565 U.S. at 415-16 (Sotomayor, J., concurring) (discussing the concerns over GPS records by noting that "the government can store such records and efficiently mine them for information years into the future") (internal citations omitted).

concurrences of Justices Alito and Sotomayor were not only concerned with the GPS monitoring of the defendant's car after a tracker was placed on it, but also with the potential of law enforcement remotely accessing a car's GPS data. Their concerns stemmed from the fact the GPS data would give the government a recorded account of everywhere that car and the individual driving it had been.[99]

It is certainly true that there are other categories of information that may give the government retrospective details about a person without implicating constitutionally protected privacy interests. To name a few, utility records,[100] pen registers,[101] and even bank records[102] can be retrieved without the government showing probable cause of a crime. However, the retrospective nature of information obtained about an individual only speaks to one aspect of the material the government is seeking. For example, a person's tax forms are not valuable solely because they provide past information about someone, but because they provide previously compiled financial disclosures from a person. Therefore, this element's use in assessing electronic surveillance is concerned with the scope of the government's intrusion. That is, whether the police have access to data about an individual that existed before they formed the suspicion to investigate them.

The importance of whether technology can reveal a tranche of historical data is expressly discussed in *Carpenter*, in subsequent Fourth Amendment cases by the lower courts, and is critical to the analysis of these issues.[103] In other cases like *Tuggle* or *Moore-Bush*, the government set up the surveillance themselves and all the data received from them was for the purpose of the investigation. Therefore, in those cases, this factor could well be absent, or analyzed differently. But for the dragnet approach of the AIR program in *Leaders of a Beautiful Struggle*, or in future cases involving facial recognition technology, it would be objectively determinable whether the technology at issue was warrantlessly deployed on the public generally and utilized later to

---

99. *See id.*; *see also id.* at 428-30 (Alito, J., concurring) (discussing the potential of long-term tracking of cellphones and other electronic devices).

100. *See* Aparna Bhattacharya, *The Impact of Carpenter v. United States on Digital Age Technologies*, 29 S. CAL. INTERDISC. L.J. 489, 498 (2020) ("Utility records traditionally received Fourth Amendment treatment similar to bank records and telephone records in that courts have found that customers do not have a reasonable expectation of privacy in such records.").

101. *See generally Smith*, 442 U.S. 735; *see also* Stephen A. Saltzburg et al., AMERICAN CRIMINAL PROCEDURE: INVESTIGATIVE - CASES AND COMMENTARY 82 (12th ed. 2022) (describing that currently under the Electronic Communications Privacy Act, 18 U.S.C. § 3121 et seq., the government does have to obtain a court order for pen registers, but the showing required is lower than probable cause).

102. *See Miller*, 425 U.S. at 442 (noting "[t]he lack of any legitimate expectation of privacy concerning the information kept in bank records").

103. *See Carpenter*, 585 U.S. at 311 (noting that over time CSLI from a cellphone can "provide[] an all-encompassing record of the holder's whereabouts," and that the "deep repository of historical location information" of CSLI opens "an intimate window into a person's life"); *see also id.* at 342 (emphasizing that unlike the situation in *Jones* "police need not even know in advance whether they want to follow a particular individual, or when" if they are using CSLI); *Leaders of a Beautiful Struggle*, 2 F.4th at 341, 344-45 (discussing how the government with relatively minimal effort could use the AIR program to compile a detailed picture of a person's habitual comings and goings around town).

gather information about a person from before they were suspected of committing a crime.

2. Extent of the Government Monitoring

The second factor of the proposed test would examine the extent of what the technology allows the government to uncover, and whether the technology used provides them with superhuman capabilities (capabilities that allow them to see, hear, and record more information than could reasonably be gathered using officers and targeted surveillance).[104] This factor was arguably a driver of the decision in *Leaders of a Beautiful Struggle*, where the AIR program gave law enforcement an enormously powerful tool to aid in their investigatory duties.[105] The Fourth Circuit drew a distinction between the AIR program and "short-term surveillance" of having humans watching a suspect by noting that the type of prolonged and precise surveillance at issue did not exist "[p]rior to the digital age."[106]

The Seventh Circuit's ruling in *Tuggle* illustrates the importance of this factor, and how a reasonable application of it in isolation can lead to the opposite conclusion from *Leaders of a Beautiful Struggle*. In *Tuggle*, the police had installed and used three cameras to monitor an outside area of the defendant's home, in an effort to uncover evidence of drug trafficking.[107] In its ruling, the court first emphasized that this was not a search because the area surveilled was knowingly exposed to the public.[108] The limited geographic and technological nature of the surveillance was a key factor in the court's decision. That is, the court said the "isolated use of pole cameras" that only captured information that would be available to any passerby on a public road by the defendant's house made the search permissible.[109] Of course, there was the issue of the *prolonged use* of these cameras, which will be discussed with the third factor *infra*.

The Seventh Circuit in *Tuggle* provided an incisive delineation of how the current regime of Fourth Amendment law in the long run will come to permit more and more surveillance by the government. The author of the opinion, Judge Flaum, began by describing in practical terms the issues that courts will be asked to confront by the ever-expanding presence of cameras and other electronic recording devices.[110] The court also recognized the fact

---

104. In reality, many techniques that the government has substantial reliance interests in such as cars and binoculars would not be included in the definition of "superhuman capabilities." The term "superhuman capabilities" is best defined as those capabilities that could only be accomplished with electronic devices that exponentially improve human capabilities of detecting, collecting, and storing information.

105. *See Leaders of a Beautiful Struggle*, 2 F.4th at 341 (explaining that "the AIR program *'tracks every movement'* of every person outside in Baltimore") (emphasis added).

106. *Id.* (quoting *Carpenter*, 585 U.S. at 310).

107. *See Tuggle*, 4 F.4th at 510.

108. *See id.* at 514.

109. *See id.* at 516-17.

110. *See id.* at 509 (describing "a future with a constellation of ubiquitous public and private cameras accessible to the government that catalog the movements and activities of all Americans").

that current Fourth Amendment doctrine is "circular[]" in the sense that as technology becomes more advanced and its use more widespread, the government will more likely evade the warrant requirement if it moves with deliberation in utilizing those technologies.[111]

In *Leaders of a Beautiful Struggle*, there is a more straightforward application of this factor. The AIR program gave the government superhuman capabilities to observe the activities of almost any citizen of Baltimore who was walking outside during its use.[112] The Fourth Circuit took pains to stretch the holding of *Carpenter* to say that the AIR program was in essence a constitutional violation of the same caliber as warrantless CSLI collection in *Carpenter*.[113] In reality, what the court was remarking upon was the fact that the AIR program was unique in that it allowed the government the ability to accomplish something they could never hope to achieve with beat cops patrolling: a photographic record of anyone within miles of the city area surveilled, eyes in the sky to catch what evades the limits of human resources.

The observations made by the judges in these cases are illustrative of the concerns this Note outlines regarding mass surveillance technologies, and why corrective action is needed. Once again, this is not to say that by using the proposed test the outcome of these cases would be different. However, it would provide a methodology to resolve complex surveillance cases that courts could consistently use and develop common law around. Moreover, it would be based on a relatively objective set of criteria that would clarify what is undoubtedly an unkempt area of law. This improvement in both efficiency and consistency would be a positive development regardless of one's opinion on how much latitude the government should have in conducting criminal investigations.

3. The Length of the Surveillance Period

The last factor of the first prong is the duration of the surveillance itself. This is perhaps the most subjective factor of the three described, seeing as the duration can be context-specific depending on when the clock starts, and the nature of the crime being investigated. However, as discussed, even simple categories of data like GPS tracking of a car have prompted concern when it is conducted for such a long period as to constitute the operational equivalent of targeting a person.[114] Justice Alito in particular remarked on the duration of surveillance in *Jones*, and while no bright line rules exist delineating how

111. *See id.* at 510 ("The upshot: the *Katz* test as currently interpreted may eventually afford the government ever-wider latitude over the most sophisticated, intrusive, and all-knowing technologies with lessening constitutional constraints.").

112. *See Leaders of a Beautiful Struggle*, 2 F.4th at 334.

113. *See id.* at 341 ("More like the CSLI in *Carpenter* and GPS-data in *Jones* than the radio-beeper in *Knotts*, the AIR program tracks every movement of every person outside in Baltimore.") (internal quotations omitted).

114. *See Jones*, 565 U.S. at 415-17 (Sotomayor, J., concurring) (suggesting citizens do not expect "that their movements will be recorded and aggregated in a manner that enables the government to ascertain" their habitual travels).

long is too long, his opinion stresses that "the line was surely crossed before the 4-week mark."[115]

While in *Tuggle* the Seventh Circuit adopted a literal interpretation of the Supreme Court's ruling in *Kyllo* that advanced technology cannot be considered a search if it's in "general public use," it did wrestle with the issue of length of observation.[116] However, the court decided that eighteen months of surveillance did not require a warrant based on probable cause, and rejected the Mosaic Theory as a basis for concluding the duration allowed the government to "piece together" the defendant's movements.[117]

The First Circuit's *en banc* opinion in *Moore-Bush* provides a clear assessment of how the length of time can matter for analyzing government action under the Fourth Amendment. The three-judge concurrence ruling that the monitoring was a search, which was written by Judge Barron, dismissed the notion that line-drawing with respect to the duration of surveillance was a fool's errand.[118] The Barron concurrence expressly relied on *Carpenter* to analogize the recording of every movement the defendant made in the surveilled front area of their house to the recording of the whole of a person's movements as captured through CSLI.[119] The concurrence in that case went on to argue that because it would be ludicrous to think the government would devote the resources to surveil a house continuously unless they were a criminal target of immense significance, the same rationale the Court recognized in *Jones* should apply, and the totality of the defendant's movements outside of their home should be given Fourth Amendment Protection.[120]

The Tenth Circuit's recent decision in *Hay*, even though it rejected the defendant's argument that the government's use of a pole camera to monitor his home was a search, recognized the importance of the duration of the monitoring to its analysis of the Fourth Amendment issue.[121] The court in that case simply said that although "the surveillance took place over an extended

115. *See id.* at 430 (internal citation omitted).

116. *See Tuggle*, 4 F. 4th at 517 (noting that "[t]he more challenging question is . . . the prolonged and uninterrupted use of . . . the pole] cameras").

117. *See id.* at 520 (noting that the Supreme Court has not required lower courts to adopt the mosaic theory).

118. *See Moore-Bush*, 36 F.4th at 357 ("[B]y relying expressly on the concurring opinions in Jones -- a case involving lengthy electronic tracking -- to conclude that there is a "reasonable expectation of privacy in the whole of [one's] movements" in public, *Carpenter was necessarily rejecting the notion that temporal line-drawing in that clearly related context is not possible.*") (emphasis added).

119. *See id.* at 333 ("[T]he Court concluded in *Carpenter*, it was reasonable for a person to expect that no such tracking was occurring as he moved about in public over a lengthy period and thus to expect that those public movements were, taken as a whole, private in consequence of the practical anonymity with respect to the whole of them that follows from the reality that virtually no one has a feasible means of piercing it.").

120. *See id.* at 334.

121. *See Hay*, 95 F. 4th at 1315 (noting that the Supreme Court in *Carpenter* "distinguished pursuing a suspect for a brief stretch, which fell within a societal expectation of privacy, from secretly monitoring and cataloguing every single movement of an individual's car for a very long period, which fell outside of it.") (internal citations omitted).

period of time," the area being monitored was public, and under current federal law no Fourth Amendment protection could be extended to it.[122]

4. Whether the Information Collected in Effect Intrudes Upon a Reasonable Expectation of Privacy the Person Would Have in a Place or Thing

It may well be the case that there will be surveillance techniques that pass muster under this test because they do not satisfy all the factors of the test above. Nevertheless, a literal application of the factors described above would not end the inquiry in every circumstance. The Supreme Court, in light of its emphasis on respecting the history and tradition of constitutional protections, has expressed support for the notion that advances in technological capabilities should not come at the cost of freedom from governmental overreach that inspired the adoption of the Fourth Amendment.[123] Even if one of the three elements from the first prong is missing, the surveillance technique would still need to satisfy the second prong of the test.

Therefore, even if a technology deployed by the government is not used to mine historical information about a person, does not give law enforcement superhuman capabilities, and is only used for a short amount of time, citizens should have a residual rule to rely on to object when their information is collected. This is the second prong of the test proposed by this Note: when a surveillance technology uncovers such a revealing category of information, either by individual collection or aggregation of that data, it has infringed on a person's expectation of privacy, and should require probable cause.

The second prong of the test is informed in large part by the analysis that was done by the Supreme Court in *Carpenter*. While it was true the result of *Carpenter* was effectively an exception to the Third-Party Doctrine, and the government's arguments were more consistent with what the Court decided in the past, there was a self-evident logic to the majority's reasoning. Namely, because of the "deeply revealing" nature of CSLI, there needed to be a baseline level of Fourth Amendment protection imposed to prevent an Orwellian reality of ubiquitous surveillance from occurring.[124]

There may well be criticism of this prong as being the *Katz* test by another name, or that it effectively swallows the multifactor test proposed. In response to this, the burden required for this prong from the objecting party will be fundamentally different than what their showing would be for the *Katz* test. A party seeking to invoke the second prong will have to show that the information collected by the government in its totality is of such a sensitive nature that no reasonable person would knowingly expose it. This is different than the *Katz* test because it allows for courts to engage in a different inquiry:

---

122. *Id.* at 316.

123. *See Jones*, 565 U.S. at 406-07 ("At bottom, we must 'assur[e] preservation of that degree of privacy against government *that existed when the Fourth Amendment was adopted.*'") (quoting Kyllo v. United States, 533 U.S. 27, 34 (2001) (emphasis added)).

124. *See Carpenter*, 585 U.S. at 320.

the question will not be whether the information in its constituent units is produced or maintained in such a way that the person cannot reasonably expect privacy over it, which is effectively what is asked under the *Katz* test. Rather, a court applying the second prong will ask whether the information when aggregated is of such a quality that the government has effectively learned information that would not be collected unless it is needed to investigate a crime. In effect, this would alter the objecting party's burden by asking them to show that the information is so private that it would only be collected if there was probable cause to believe the person had committed a crime and was under investigation. While making this type of showing would be difficult for an objecting party to demonstrate, it would effectively help prevent the government from maintaining stores of data on people not suspected of crimes, which could help preempt many issues related to facial recognition technology, metadata, and other forms of electronically stored information.

This prong would reset the balance of interests and make the inquiries by courts more straightforward. Such a balance would be an improvement over the assortment of rules and exceptions that make up the current and dizzying state of Fourth Amendment law. Therefore, the test proposed by this Note should be considered, as it would work towards clearing up an area of law that needs reform.

IV. CONCLUSION

The Fourth Amendment exists to ensure American citizens maintain a baseline amount of privacy in their person and effects by restricting the government's ability to conduct searches and seizures of property, whether digital or not. We are living through an age where law enforcement is continually gaining an expansive technological capability to collect, analyze, and utilize electronic data to investigate, solve, and prosecute crime. This will only accelerate with the continued advancement of artificial intelligence systems that can both collect vast amounts of data with ease, and automatically perform analytical tasks using that data. While these advancements have yielded positive results in achieving public safety objectives, there have been serious costs to the privacy of American citizens.

What the right balance between these objectives is depends on policy many factors, but the Supreme Court and lower courts need to ensure that there is a baseline level of Fourth Amendment protection against new methods of surveillance. Adopting the test proposed in this Note is not a panacea to resolving the complex legal, practical, and philosophical problems posed by electronic surveillance. However, it is a step in the right direction by seeking to provide rules that aim to balance the considerable authority the government wields with the freedom from unreasonable searches and seizures guaranteed in the Constitution.