I Spy with My Many Eyes: The Government's Unbridled Use of Your Surveillance Cameras

BRIAN A. WEIKEL[†]

Surveillance cameras are increasingly used by the public and law enforcement to prevent and prosecute criminal activity. Individuals and companies can grant law enforcement access to private cameras for both live monitoring feeds and recorded footage, thereby creating a quasi-public network of private cameras. According to the third-party doctrine, the government can access all information from these surveillance cameras without a subpoena or warrant and without infringing upon Fourth Amendment privacy protections. However, as technology advances and the prevalence of surveillance cameras rises, this per se rule fails to account for one's reasonable expectation of privacy in the public and private spheres.

This Note examines the 2022 San Francisco ordinance, which authorizes the government to use private cameras in a wide variety of circumstances. Specifically, it reviews the ordinance through the mosaic theory, whose proponents champion as a necessary correction to the erosion of Fourth Amendment rights and whose opponents condemn as doctrinally flawed and impractical to administer. To address the theory's doctrinal shortcomings, this Note reviews the historical development of privacy protections with each new technology considered by the Supreme Court. To demonstrate how the theory may be applied to other technologies, this Note analyzes the circuit court split on whether the warrantless use of pole cameras constitutes a search under the Fourth Amendment. Pole cameras serve as a useful proxy for private cameras under the ordinance.

Ultimately, this Note recommends that the San Francisco ordinance be modified to safeguard an individual's reasonable expectation of privacy by adding a notice requirement with camera stickers and adjacent signs, requiring police officers to provide camera owners with a brief descriptive justification for each requested video, and limiting the duration of access to live and historical feeds for each event.

[†] J.D. Candidate 2024, University of California College of the Law, San Francisco; Executive Notes Editor, *UC Law Journal*, Volume 75. Thank you to Adjunct Professor Wesley Cheng for his brilliant insight throughout the research and writing of this Note; Senior Notes Editors Rafi Bortnick, Bob Chan, Max Joachim, Kristie Lam, and Thomas McCarthy for their dedication; and my family and partner for their unyielding support.

TABLE OF CONTENTS

INTRODUCTION

Cities and foreign countries are turning to comprehensive surveillance tools to combat terrorism and crime.[1] San Francisco is no exception. The city recently passed an ordinance, which allows law enforcement to tap into a vast network of private cameras to supplement its policing tools.[2] This is an expansive addition to the traditional tools like subpoenas and search warrants that allow law enforcement to obtain information.[3]

On May 17, 2022, San Francisco Deputy City Attorney Zachary Porianda proposed a modified ordinance that would authorize the "use [of] surveillance cameras and surveillance camera networks owned, leased, managed, or operated by non-City entities."[4] According to the San Francisco Police Department ("SFPD"), the modified Surveillance Technology Policy ("STP")'s authorization of temporary live monitoring would help officers manage events with public safety concerns such as sideshows.[5] The STP may help law enforcement monitor in-progress criminal activity and review camera footage

1. *See, e.g.*, Ali Watkins, *How the N.Y.P.D. Is Using Post-9/11 Tools on Everyday New Yorkers*, N.Y. TIMES (Sept. 8, 2021), https://www.nytimes.com/2021/09/08/nyregion/nypd-9-11-police-surveillance.html (last updated June 22, 2023); Rick Rojas, *In Newark, Police Cameras, and the Internet, Watch You*, N.Y. TIMES (June 9, 2018), https://www.nytimes.com/2018/06/09/nyregion/newark-surveillance-cameras-police.html; Isabelle Qian, Muyi Xiao, Paul Mozur & Alexander Cardia, *Four Takeaways From a Times Investigation Into China's Expanding Surveillance State*, N.Y. TIMES, https://www.nytimes.com/2022/06/21/world/asia/china-surveillance-investigation.html (July 26, 2022); Paul Mozur, Adam Satariano, Aaron Krolick, Aliza Aufrichtig *'They Are Watching': Inside Russia's Vast Surveillance State*, N.Y. TIMES (Sept. 22, 2022), https://www.nytimes.com/interactive/2022/09/22/technology/russia-putin-surveillance-spying.html.

2. S.F., CAL., ADMIN. CODE ch.19B (2022); *Regular Meeting Before S.F. Bd. of Supervisors* (Sept. 27, 2022) [hereinafter Bd. of Supervisors Meeting Minutes, Sept. 27, 2022], https://sfbos.org/sites/default/files/bag092722_minutes.pdf; Nellie Bowles, *Why Is a Tech Executive Installing Security Cameras Around San Francisco?*, N.Y. TIMES, https://www.nytimes.com/2020/07/10/business/camera-surveillance-san-francisco.html (July 13, 2020); JENNIFER KING, DEIRDRE K. MULLIGAN & STEVEN P. RAPHAEL, CITRIS REPORT: THE SAN FRANCISCO COMMUNITY SAFETY CAMERA PROGRAM 11 (2008) (finding that pole cameras are not as effective as politicians propose them to be, based on an analysis of the Community Safety Camera (CSC) program passed by the S.F. Board of Supervisors in 2006).

3. Subpoenas are court orders (or administrative orders issued by a government agency) requiring a person to appear and testify in court (or to an agency) or to bring forth certain documents including metadata for electronic mediums. FED. R. CIV. P. 45. Search warrants are written court orders that grant law enforcement the right to search a defined area and seize property specifically described or located in the warrant including the content or actual information sought for electronic mediums. *See In re* Grand Jury Subpoenas Dated Dec. 10, 1987, 926 F.2d 847, 854 (9th Cir. 1991) ("Subpoenas are not search warrants. They involve different levels of intrusion on a person's privacy. A search warrant allows the officer to enter the person's premises, and to examine for himself the person's belongings. The officer, pursuant to the warrant, determines what is seized.").

4. S.F. County, Cal., Ordinance No. 205-22, Ordinance Approving Surveillance Technology Policy for Police Department Use of Non-City Entity Surveillance Cameras (Nov. 6, 2022); *see also* ADMIN. ch. 19B § 1–2 (noting that the proposal did not modify the local administrative code).

5. *Non-City Entity Surveillance Camera Policy Ordinance: Hearing on SF Admin Code 19B Before Police Comm.* (Sept. 12, 2022), at 4 [hereinafter Police Presentation, Sept. 12, 2022], https://sfgov.legistar.com/View.ashx?M=F&ID=11229458&GUID=3E210DEF-8160-4CBD-97C8-BC89097FCCE0. Sideshows, events when (typically) young people block traffic to intentionally spin and burn a car's rear tires to leave donut or cursive patterns on the pavement, are becoming more frequent since the start of the pandemic. Bradley Berman, *In Street Takeovers, Young Stunt Drivers Outmaneuver the Police*, N.Y. TIMES (Sept. 4, 2022), https://www.nytimes.com/2022/09/04/business/stunt-driving-sideshows.html?searchResultPosition=1.

when AMBER or SILVER alerts are issued.[6] The SFPD also touted how historical footage aids investigators to identify and remove violent offenders from the public.[7]

In response, prominent organizations, such as the Bar Association of San Francisco, raised alarms over the mass surveillance of the public because the policy is indiscriminate, vague, and otherwise violates the Fourth Amendment rights of residents and visitors.[8] Some organizations sued the SFPD for violating the existing policy by accessing a private surveillance camera network "to spy on demonstrators protesting the 2020 police murder of George Floyd."[9] They noted the department's "history of spying on marginalized groups and political dissents."[10] Email exchanges between the SFPD and the Union Square Business Improvement District ("BID"), a private non-profit organization with authority to collect taxes and provide street cleaning and other services, revealed that the police "requested and received a 'data dump' of 12 [continuous] hours of footage from every camera in the [district] . . . without any kind of specificity" and the Homeland Security Unit separately requested forty-eight hours of real-time access to the surveillance network.[11] The BID granted the requests for remote access to the live feed and extended law enforcement's access to nine days.[12]

Nonetheless, the Board of Supervisors passed the ordinance in a seven-to-four vote on September 27, 2022.[13] The mayor approved the ordinance shortly thereafter.[14]

---

6. *See Non-City Entity Surveillance Camera Policy Ordinance: Hearing on SF Admin Code 19B Before Police Comm.* (July 11, 2022), at 4–6, [hereinafter Police Presentation, July 11, 2022], https://sfgov.legistar.com/View.ashx?M=F&ID=11053200&GUID=C65D52A6-C3F8-4E2D-BFFE-0825E1A7BBEB; *Regular Meeting of Rules Comm. Before S.F. Bd. of Supervisors* (July 11, 2022) [hereinafter Rules Comm. Meeting Minutes, July 11, 2022], https://sfgov.legistar.com/View.ashx?M=M&ID=986966&GUID=26C0BC85-A74A-4527-9C7D-11838A74F562. AMBER alerts are issued for child abduction, violet criminals posing an imminent threat, or missing and endangered persons; SILVER alerts are issued for individuals with intellectual disabilities, dementia, or other cognitive impairments. *Alerts Save Lives: A Unified Message Regarding the Need to Support Nationwide Alerts*, BUREAU JUST. ASSISTANCE (2018), https://bja.ojp.gov/library/publications/alerts-save-lives-unified-message-regarding-need-support-nationwide-alerts.

7. *See* Police Presentation, July 11, 2022, *supra* note 6; Rules Comm. Meeting Minutes, July 11, 2022, *supra* note 6; Police Presentation, Sept. 12, 2022, *supra* note 5, at 6–8.

8. *See, e.g.*, Email from Bar Ass'n of S.F., to S.F. Bd. of Supervisors (Sept. 1, 2020), *as reprinted in* Board of Supervisors Agenda Packet 092722 at 437–43; Email from City & Cnty S.F. Police Dep't, to S.F. Bd. of Supervisors (Sept. 9, 2022), *reprinted in* Board of Supervisors Agenda Packet at 15–19.

9. *See, e.g.*, Press Release, Elec. Frontier Found., EFF & ACLU Brief: SFPD Violated Surveillance Law by Spying on Protests for Black Lives (Aug. 15, 2022), https://www.eff.org/press/releases/eff-aclu-brief-sfpd-violated-surveillance-law-spying-protests-black-lives.

10. Brief for Petitioners-Appellants at 12–13, Williams v. San Francisco, 2023 WL 3815182 (No. A165040).

11. Dave Maass & Matthew Guariglia, *San Francisco Police Accessed Business District Camera Network to Spy on Protestors*, ELEC. FRONTIER FOUND. (July 27, 2020), https://www.eff.org/deeplinks/2020/07/san-francisco-police-accessed-business-district-camera-network-spy-protestors.

12. *Id.*

13. Bd. of Supervisors Meeting Minutes, Sept. 27, 2022, *supra*, note 2, at 7.

14. S.F., Cal., Ordinance No. 220606, Surveillance Technology Policy for Police. Department Use of Non-City Entity Surveillance Cameras (Oct. 6, 2022).

The enacted STP authorizes three non-exclusive uses for live monitoring or historical footage.[15] First, police may "temporarily live monitor activity during exigent circumstances, significant events with a public safety concern, and investigations relating to active misdemeanor and felony violations."[16] Exigent circumstances involve an immediate danger of death or serious physical injury, or scenarios when "crowd sizes or other issues creat[e] imminent public safety hazards."[17] Alternatively, with "credible information of criminal activity," any high-ranked police officer can request live monitoring to investigate "specific criminal activity."[18] Second, police can obtain historical footage to gather evidence relevant to "a specific criminal investigation."[19] Third, police can obtain historical footage to gather evidence relevant to "an internal investigation regarding officer misconduct."[20] Consequently, police may automatically access—without subpoena or warrant—historical videos, images, and other data without substantial participation from the private camera's owner.[21]

The constitutionality of the government's use of private cameras remains unclear post-*Carpenter v. United States*, especially when express consent is given by an organization managing the surveillance system rather than its individual members. In *Carpenter,* the Supreme Court's held that the Government generally must obtain a search warrant supported by probable cause for "personal location information maintained by a third party."[22] Following the landmark ruling, circuit courts are split on the methodology needed to determine whether warrantless, long-term surveillance of residences from pole cameras constitutes a search under the Fourth Amendment.[23] The United States Court of Appeals for the Seventh Circuit held that the government's prolonged use of pole cameras was not a search, thus no warrant was required.[24] Conversely, in another case, the United States Court of Appeals for the First Circuit overturned the district court ruling that would have suppressed similar evidence, but the en

15. *See* S.F. POLICE DEP'T, SURVEILLANCE TECHNOLOGY POLICY, Bd. of Supervisors 205-22, at 2 (2002) [hereinafter Non-City STP], https://sfgov.legistar.com/View.ashx?M=F&ID=11308461&GUID=3413B582-95F4-4B4C-A146-1919CEEAAEB7.

16. *Id.*

17. ADMIN. § 19B.1; Non-City STP, *supra* note 15, at 2.

18. Non-City STP, *supra* note 15, at 2.

19. *Id.*

20. *Id.*

21. No private search is necessarily performed by the camera owner. *See* United States v. Jacobsen, 466 U.S. 109, 120 (1984) (noting that under the private search doctrine—authorized or not—eviscerated an individual's reasonable expectation of privacy, so the government's duplication of that search does not violate a person's privacy).

22. Carpenter v. United States, 138 S. Ct. 2206, 2214, 2221 (2018).

23. Generally, pole cameras are defined as surveillance cameras that are often attached to utility poles, but they can sometimes be secured to the building or corridor walls or the tops of vehicles. ANNE TOOMEY MCKENNA & CLIFFORD S. FISHMAN, WIRETAPPING & EAVESDROPPING § 30:84 (3d ed. 2022).

24. United States v. Tuggle, 4 F.4th 505, 523–24 (7th Cir. 2021), *cert. denied*, 142 S. Ct. 1107 (2022).

banc panel of six judges was evenly split on whether the government's actions constituted a search.[25]

Absent any binding circuit court authority, the City and County of San Francisco may be deputizing private individuals and entities to act as extensions of the government with or without the express consent of the camera owners.[26] The question remains: Does the STP make private cameras, which are perpetually pointed at the city's homes, businesses, and their surrounding areas, functionally government pole cameras?

In Part I, this Note begins by reviewing the mosaic theory's doctrinal underpinnings through the Supreme Court's review of new technologies.

In Part II, the application of the mosaic theory is presented through the circuit court split on the warrantless use of private cameras' closest proxy, specifically pole cameras.

In Part III, three core issues undermining the constitutionality of the STP are presented. First, the prolonged, continuous nature of cameras that are pointed at homes makes videos deeply revealing. Second, the ordinance creates a mass surveillance network due to its depth, breadth, and comprehensive reach to all residents and visitors. Third, the wide latitude with which law enforcement may access cameras in real-time, the duration of each granted access, and the recording capabilities of many cameras make police's collection of information inescapable and automatic. Although the STP is likely constitutionally sufficient, this Note provides three recommendations to protect an individual's reasonable expectation of privacy while retaining efficient access to cameras for law enforcement's investigations.

I. THE DEVELOPMENT OF THE MOSAIC THEORY

Justice Scalia's approach to the Fourth Amendment cases is more widely appreciated than his other work because he applied a mixture of common law and originalism.[27] A review of Fourth Amendment jurisprudence, through this lens, proves instructive for the theoretical and practical implications of adopting the mosaic theory.[28]

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[29] The language that follows describes the procedure for obtaining a

25. United States v. Moore-Bush, 36 F.4th 320, 321 (1st Cir. 2022) (en banc) (per curiam), *cert. denied*, 143 S. Ct. 2494 (2023).

26. *But see* Skinner v. Ry. Lab. Execs.' Ass'n, 489 U.S. 602, 614 (1989) ("Whether a private party should be deemed an agent or instrument of the Government for Fourth Amendment purposes necessarily turns on the degree of the Government's participation in the private party's activities.").

27. *See* Brandon R. Teachout, *On Originalism's Originality: The Supreme Court's Historical Analysis of the Fourth Amendment from* Boyd *to* Carpenter, 55 TULSA L. REV. 63, 64, 107 (2019).

28. *See* Orin S. Kerr, *The Curious History of Fourth Amendment Searches*, 2012 SUP. CT. REV. 67, 69 (2012).

29. U.S. CONST. amend. IV.

valid warrant.[30] Thus, if the government's investigation was not a search, then the conduct fell outside the purview of the Fourth Amendment.[31] If the government's investigation was a Fourth Amendment search, the government "presumptively required a warrant."[32] For most of the twentieth century, the Supreme Court supported the "warrant preference view" where the presence of a warrant substantially affected the search's validity.[33] Under the warrant preference principle, if a government officer secures judicial authorization for a search by warrant or an exception to the warrant requirement applies, the search will be presumed reasonable.[34]

Early courts focused Fourth Amendment search inquiries on whether one's property rights were interfered with, which primarily asked whether the government physically trespassed.[35] This trespass-like standard continued until *Katz v. United States*, in which Justice Harlan's concurrence established the privacy test.[36] Several decades later, in *United States v. Jones*, the Supreme Court returned to the "common-law trespassory test" by setting property rights as the baseline for initial Fourth Amendment inquiries.[37] The concurring opinions penned by Justices Alito and Sotomayor acknowledged the mosaic theory and breathed fresh air into the debate over how surveillance techniques and tools should be analyzed in future Fourth Amendment cases.[38]

Shortly thereafter, Supreme Court issued its landmark decision in *Carpenter v. United States*, which identified the deeply revealing nature of the information sought, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection as factors that warrant Fourth Amendment protection.[39] By *adding* factors to a holistic rather than elemental test, the Court effectively endorsed the mosaic theory of privacy.[40] The mosaic theory analyzes the aggregations of information collected by the government for

30. *Id.*

31. Nicholas A. Kahn-Fogel, *Katz, Carpenter, and Classical Conservatism*, 29 CORNELL J.L. & PUB. POL'Y 95, 99 (2019).

32. *Id.*

33. *See* Cynthia Lee, *Reasonableness with Teeth: The Future of Fourth Amendment Reasonableness Analysis*, 81 MISS. L.J. 1133, 1138 (2012). *But see* Kit Kinports, *The Origins and Legacy of the Fourth Amendment Reasonableness-Balancing Model*, 71 CASE W. RES. L. REV. 157, 162 (2020) (describing the Supreme Court's abandonment of the warrant-presumption model in *United States v. Knights*, *Samson v. California*, and *Maryland v. King*).

34. *See* Lee, *supra* note 33, at 1138.

35. *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 816 (2004).

36. *See* Kerr, *supra* note 28, at 67–68.

37. *See* United States v. Jones, 565 U.S. 400, 409 (2012); Kerr, *supra* note 28, at 68 (noting that the Court "revived" the trespass test); Nicholas A. Kahn-Fogel, *Property, Privacy, and Justice Gorsuch's Expansive Fourth Amendment Originalism*, 43 HARV. J.L. & PUB. POL'Y 425, 428 (2020) (noting that the Court "resuscitated the old trespass test").

38. *See* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 313–14, 326–28, 333–36 (2012).

39. Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018).

40. Paul Ohm, *The Many Revolutions of Carpenter*, 32 HARV. J.L. & TECH. 357, 373 (2019).

a particular person rather than looking at the isolated steps in the collection process.[41] Although the mosaic theory is commonly applied to the reasonable expectation of privacy test, the theory may be applied to the overarching Fourth Amendment search doctrine, which includes the trespass-like test.[42] Its stalwarts and critics must decide whether the language found in Supreme Court precedent is literally limiting or defines the parameters of a categorical test.[43] The mosaic theory may flexibly extend a person's privacy rights for each technology and its variant in an era without the need to readjust the test to achieve equilibrium between the Government and the individual.[44]

In this Part, I propose that the expansive definition of a "search" evidences the role of privacy in determining reasonableness for the physical intrusion and reasonable expectation of privacy tests. Its developmental shift in scope reflects the Supreme Court's attempt to strike a workable balance between individual privacy and government interests, absent subpoenas or search warrants. Further, I claim that the essential components of the mosaic theory are indicated not only in *Jones* and *Carpenter* but also in their precursors. The mosaic theory protects more than a person's reasonable expectation of privacy in their movements. It counteracts the erosion of Fourth Amendment rights by new surveillance tools and techniques.

A. THE PHYSICAL INTRUSION ONTO MOSAIC FLOORS

Since 1886, the Supreme Court has viewed the Fourth Amendment's scope as being about privacy.[45] The Supreme Court never restricted "search" to physical trespass alone.[46] When analyzing the facts and circumstances of Fourth Amendment issues, the Court seemingly has swung between the traditional sequential approach and the collective approach embodied in the mosaic theory.

---

41. Although the mosaic theory is frequently applied to the reasonable expectation of privacy test, it may be applied to the broader Fourth Amendment search doctrine, which includes the trespass test. *See* Kerr, *supra* note 38, at 313–14, 326–28, 333–36 (discussing the aggregation of facts and circumstances examined in Fourth Amendment search cases).

42. *See Carpenter*, 138 S. Ct. at 2213; Kerr, *supra* note 38, at 320–21. See also *infra* Parts III.A and III.B for discussion of the trespass and reasonable expectation of privacy tests, respectively.

43. *Compare* United States v. Moore-Bush, 36 F.4th 320, 331 (1st Cir. 2022) (en banc) (Barron, C.J., Thompson & Kayatta, JJ., concurring) (using precedent to define each element of the mosaic theory as a fluid categorical test) *with id.* at 361 (Lynch, Howard & Gelpí, JJ., concurring) (recognizing its constraint from the plain meaning of the language to reject the mosaic theory) *and with* United States v. Tuggle, 4 F.4th 505, 510–11 (7th Cir. 2021) (using precedent to distinguish the elements and reject the mosaic theory).

44. *See generally* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476 (2011) (describing the correction mechanism of Fourth Amendment jurisprudence).

45. Orin S. Kerr, Katz *As Originalism*, 71 DUKE L.J. 1047, 1061 (2022).

46. *See* Kyllo v. United States, 533 U.S. 27, 32 (2001) ("When the Fourth Amendment was adopted, as now, to 'search' meant '[t]o look over or through for the purpose of finding something; to explore; to examine by inspection.'") (alteration in original); Kerr, *supra* note 28, at 77.

1. Boyd v. United States*: Papers*

In *Boyd v. United States*, investigators obtained an order, which required Boyd to provide the Government with an invoice, to determine whether Boyd paid taxes on imported items.[47] The Court held that forced compliance with the Government's order was a Fourth Amendment search and seizure because it contained the Fourth Amendment's "substance and essence, and effects their substantial purpose" though no "forcible entry into a man's house and search[] amongst his papers" occurred. [48] The "papers" served as a proxy for the document's contents rather than its mere existence because of the focus of the search.[49] Further, the Court held that the Fourth Amendment applies to "all invasions" by the Government into "the sanctity of a man's home and the *privacies* of life."[50] The Government's search into business records rather than a diary implies that privacy protections extend beyond "personal information" that is "revealing" to "privately held, but not overtly intimate information," such as daily habits involuntarily captured on camera.[51] Until *Olmstead v. United States*,[52] the Court did not explicitly separate "search" from "trespass."[53]

2. Olmstead v. United States*: Wiretap*

In *Olmstead*, the Court used originalism to define "search" within Fourth Amendment jurisprudence.[54] Prohibition agents wiretapped Roy Olmstead's telephone lines outside his home and office to collect evidence of his role as a ringleader of a bootlegging operation. The Court held that the Government's actions did not constitute a Fourth Amendment search or seizure[55] and "no entry" occurred because the agents inserted wires on public property.[56] Even if houses, papers, and effects were "liberally construed," the eavesdropping did not fall neatly into any of those protected categories because the evidence was

47. Boyd v. United States, 116 U.S. 616, 635 (1886).

48. *Id.* at 618.

49. *See* Andrew Guthrie Ferguson, *The "Smart" Fourth Amendment*, 102 CORNELL L. REV. 547, 569 (2017).

50. *Id.* (emphasis added).

51. *See id.*

52. *See generally* Olmstead v. United States, 277 U.S. 438 (1928), *overruled by* Berger v. New York, 388 U.S. 41 (1967) *and* Katz v. United States, 389 U.S. 347 (1967).

53. *See, e.g.*, United States v. Lee, 274 U.S. 559, 563 (1927); Perlman v. United States, 247 U.S. 7, 14–15 (1918); Hale v. Henkel, 201 U.S. 43, 80–81, (1906) (McKenna, J., concurring), *overruled by* Murphy v. Waterfront Comm'n of N.Y. Harbor, 378 U.S. 52, 74 (1964); *see also* Kerr, *supra* note 28, at 80–81 (describing the shift in what constituted a search).

54. *See, e.g.*, *Olmstead*, 277 U.S. at 463 ("The well-known historical purpose of the Fourth Amendment . . . was to prevent the use of government force to search a man's house, his person, his papers, and his effects."); Carroll v. United States, 267 U.S. 132, 149 (1925) (citing Boyd v. United States, 116 U.S. 616, 623 (1886)) ("The Fourth Amendment is to be construed in the light of what was deemed an unreasonable search and seizure when it was adopted."); *see also* Lawrence Rosenthal, *An Empirical Inquiry into the Use of Originalism: Fourth Amendment Jurisprudence During the Career of Justice Scalia*, 70 HASTINGS L.J. 75, 85–86 (2018) (noting originalism's roots in Fourth Amendment precedent).

55. *See Olmstead*, 277 U.S. at 455, 466.

56. *See id.* at 456–57, 464.

"secured by the use of the sense of hearing and that only."[57] For four decades thereafter, courts used the "actual physical invasion" standard for a search before a Fourth Amendment violation could be found.[58]

3. Goldman v. United States*: Detectaphone*

In *Goldman v. United States*, the Court again declined to directly link "trespass" to "search" under the Fourth Amendment.[59] Martin Goldman, who was suspected of conspiracy to violate the Bankruptcy Act, argued that federal agents physically intruded when they broke into his office and installed a detectaphone, a sensitive listening apparatus that amplifies sound waves received by a wire, in the partition wall.[60] Since the microphone did not work, federal agents affixed a more sensitive microphone to the wall of an adjoining office.[61] The Court rejected the theory of tainted evidence because the form of electronic eavesdropping did not fit squarely within the wiretapping statute.[62] The facts suggested that the alleged "trespass did not aid materially in the use of the [sensitive microphone]."[63] The Court held that the use of the sensitive microphone was not a Fourth Amendment search because the case could not be sufficiently distinguished from *Olmstead*.[64] Consequently, the early twentieth century electronic eavesdropping technologies largely fell into the regulatory gap for relatively unrestricted use by law enforcement.[65]

Yet, scholars note that the Court's sparing use of "trespass" in *Olmstead* and subsequent cases was intended to broaden the definition of searches beyond physical intrusions.[66] Nonetheless, the Court's ruling in *Katz v. United States* perpetuated the notion that *Olmstead* and *Goldman* created the "trespass

57. *See id.* at 464–65.

58. *See id.* at 466; Renée McDonald Hutchins, *Tied Up in Knotts? GPS Technology and the Fourth Amendment*, 55 UCLA L. REV. 409, 425 (2007).

59. *See* Goldman v. United States, 316 U.S. 129, 134–35 (1942), *overruled by* Katz v. United States, 389 U.S. 347 (1967).

60. *See id.* at 131, 134.

61. *See id.* at 131–32.

62. Federal Communications Act of 1934, ch. 652, Title VI § 605, 48 Stat. 1064, 1103–04 (1934) (current version at 47 U.S.C. § 605); Robert A. Pikowsky, *The Need for Revisions to the Law of Wiretapping and Interception of Email*, 10 MICH. TELECOMM. & TECH. L. REV. 1, 29 (2003).

63. *See Goldman*, 316 U.S. at 135.

64. *See id.*

65. *See* Pikowsky, *supra* note 62, at 29.

66. *See, e.g.*, Michael J. Zydney Mannheimer, *Decentralizing Fourth Amendment Search Doctrine*, 107 KY. L.J. 169, 178 (2019) (noting that in the pre-*Katz* era, the Court applied "a general trespass-like analysis, not the actual law of trespass"); Kiel Brennan-Marquez & Andrew Tutt, *Offensive Searches: Toward A Two-Tier Theory of Fourth Amendment Protection*, 52 HARV. C.R.-C.L. L. REV. 103, 110–11 (2017) (noting that in *Florida v. Jardines*, 569 U.S. 1 (2013), the majority "consciously crafted to evade . . . trespass[]" and opted for "physical intrusion"); William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 HARV. L. REV. 1821, 1835–36 (2016) (noting that Justice Scalia avoided trespass, "instead reasoning in the abstract"); Kerr, *supra* note 28, at 82 (using "trespass" to distinguish *Hester v. United States*, 265 U.S. 57 (1924) from *United States v. Lee*, 274 U.S. 559 (1927)).

doctrine"[67] while temporarily departing from originalism—that is, analysis relying on historical evidence of the Fourth Amendment as prevention against *any* government force.[68] Since *Katz*, the Court largely ignored the trespass-like standard before unexpectedly reviving it in *United States v. Jones*.[69] Therefore, within the property-based approach, courts need not restrict "search" to the government's attempts to obtain information in an isolated trespass, but courts may view it within the broad search for evidence.[70] For example, under *Goldman*, the seemingly innocuous use of one private camera by law enforcement may be viewed as part of an overarching search within a surveillance network.

4. United States v. Jones*: Global Positioning System Tracker*

In *Jones*, government agents suspected Antoine Jones and Lawrence Maynard of conspiring to traffic narcotics.[71] The agents subsequently obtained a warrant to install a Global Positioning System ("GPS") tracker on the sports utility vehicle ("SUV") that was registered to Jones's spouse.[72] The warrant allowed the agents to place the tracker on the SUV in the District of Columbia within ten days.[73] The agents affixed the device to the SUV's underside in Maryland on the eleventh day.[74] For twenty-eight days, the Government tracked the SUV's movements with accuracy ranging from 50 to 100 feet of the vehicle's actual location.[75] Jones' and Maynard's appeals were consolidated, but Jones independently argued that the evidence obtained through the GPS tracker violated his Fourth Amendment rights.[76]

The Supreme Court held that a Fourth Amendment search occurs when the government physically intrudes upon a constitutionally protected area to obtain information.[77] Under a return to an originalist interpretation, Justice Scalia, writing for the majority, held that the attachment of the GPS tracker to the SUV was trespassing because the Government "physically occupied private

67. *See* Kerr, *supra* note 28, at 87. *But see* Ricardo J. Bascuas, *The Fourth Amendment in the Information Age*, 1 VA. J. CRIM. L. 481, 487–89 (2013) (alluding that *Olmstead* did not create the trespass doctrine because the *Katz* reasonable-expectation-of-privacy test was added to a property-based principle that would have resulted in a contrary outcome in *Olmstead*).

68. *See* Rosenthal, *supra* note 60, at 86.

69. *See* United States v. Jones, 565 U.S. 400, 405, 409 (2012) (noting that, following *Olmstead*, the Court has "deviated from that exclusively property-based approach" because "the *Katz* reasonable-expectation-of-privacy test has been *added to,* not *substituted for,* the common-law trespassory test"); *see also* Kerr, *supra* note 28, at 68 n.5 ("This came as a surprise to every student and scholar of the Fourth Amendment.").

70. *See* Kerr, *supra* note 28, at 320.

71. *See* United States v. Maynard, 615 F.3d 544, 548 (D.C. Cir. 2010), *aff'd in part sub nom.* United States v. Jones, 565 U.S. 400 (2012).

72. *See Jones*, 545 U.S. at 402–03.

73. *See id.*

74. *See id.* at 403.

75. *See id.*

76. *See Maynard*, 615 F.3d at 548–49; *Jones*, 545 U.S. at 403.

77. *See Jones*, 545 U.S. at 407–08, 408 n.5.

property."[78] Justice Scalia concluded that the Fourth Amendment's drafters would have classified the attachment of the GPS tracker as a "'search' within the meaning of the Fourth Amendment when it was adopted."[79] With "faint-hearted" originalism, Justice Scalia sought to protect the privacy protections of 1791, regardless of modern electronic surveillance techniques under the physical trespass standard.[80] Although the Court's decision was unanimous, five other justices wrote or joined separate concurrences to point out the dissonance with modern surveillance methods.[81] Where Justice Scalia stopped short of a comprehensive reasonable expectation of privacy analysis, the five concurring justices leaned into the mosaic theory, which the Court of Appeals for the District of Columbia Circuit advanced in *United States v. Maynard*.[82]

In *Maynard*, the D.C. Circuit analyzed the Government's actions in two steps: "first whether that use of the device was a search and then, having concluded it was, consider whether it was reasonable and whether any error was harmless."[83] For the first step, the D.C. Circuit suggested that the Government's actions amounted to "dragnet-type law enforcement practices," and that the Supreme Court sought to protect against warrantless "twenty-four hour surveillance."[84] The *Maynard* court analyzed the use of the GPS tracker under "different constitutional principles," and then rejected the Government's argument that the *United States v. Knotts*'s public observation doctrine was controlling.[85]

---

78. *See id.* at 404–05 (holding that the Government affixed the GPS tracker to a person's effect was sufficient, or its use was not necessarily required).

79. *See id.*

80. *See* Robert M. Bloom & Eliza S. Walker, *Rules and Standards in Justice Scalia's Fourth Amendment*, 55 U. RICH. L. REV. 713, 720 (2021).

81. *See Jones*, 565 U.S. at 414–15, 425, 428–31. Justices Breyer, Ginsburg, Kagan and Alito posited that police using unmarked cars and aerial surveillance to follow a car may evade the purview of the Fourth Amendment, whereas Justice Sotomayor separately wrote that "physical intrusion is now unnecessary to many forms of surveillance." *Id.*

82. *See* Kerr, *supra* note 28, at 326; *Maynard*, 615 F.3d at 561–65.

83. *Maynard*, 615 F.3d at 555.

84. *See id.* at 556–57; *see also* United States v. Knotts, 460 U.S. 276, 283–84 (1983) (holding that "[a] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another," but leaving open the question of whether constant surveillance requires a warrant).

85. Under the public observation doctrine, individuals do not have a reasonable expectation of privacy in anything exposed to public view. *See* 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, 394 (2013); *Maynard*, 615 F.3d at 556–58 ("'[W]holesale' or 'mass' electronic surveillance of many individuals requires a warrant."); California v. Ciraolo, 476 U.S. 207, 213–14 (1986) ("Any member of the public flying in this airspace who glanced down could have seen everything that these officers observed."); *Knotts*, 460 U.S. at 284 ("[I]f such dragnet-type law enforcement practices as respondent envisions should eventually occur, then there will be time enough then to determine whether different constitutional principles may be applicable."). *Cf.* Collins v. Virginia, 138 S. Ct. 1663, 1672 (2018) (holding that under the plain view doctrine, an individual does not benefit from Fourth Amendment protection where an officer has a prior justification for an intrusion into a constitutionally protected area, activity, or object itself and discovers incriminating evidence during the course of that intrusion); Hester v. United States, 265 U.S. 57, 59 (1924) (holding that under the open fields doctrine,

Beyond an aversion to prolonged surveillance of a single person, the D.C. Circuit focused on whether Jones "exposed" the information that was the subject of the search to the public.[86] In terms of "actual" exposure, the court held that "the likelihood a stranger would observe all those movements is not just remote, it is essentially nil."[87] The D.C. Circuit broke with conventional Fourth Amendment law when reviewing Jones's "constructive" exposure.[88] Rather than analyzing each type of information that would be exposed to the public, the *Maynard* court reviewed the "whole of [Jones's] movements over the course of a month."[89] The court concluded that "prolonged surveillance of a person's movements may reveal an intimate picture of [their] life."[90] The collected information revealed by twenty-eight days of GPS tracking was more akin to "a single clearinghouse of information" for one individual than the public records on the same individual compiled by local government services scattered across the country.[91] According to the D.C. Circuit, the length of the monitoring itself would necessarily reveal "an intimate picture of the subject's life that [they] expect no one to have," thus implicating the Fourth Amendment.[92]

In his concurrence in *Jones*, Justice Alito agreed with the majority only in judgment, and framed the "various and varying considerations" within the *Katz* test like the D.C. Circuit.[93] Justice Alito found Justice Scalia's physical intrusion test that focused on the installation of the GPS device on the car far too attenuated from the language of the Fourth Amendment.[94] Instead, Justice Alito emphasized time as a factor of reasonableness.[95] First, if the mere attachment of the GPS tracker to a car amounted to trespass, then the duration for which it was attached to the car and its use, would be irrelevant. Second, Justice Alito recognized that extensive surveillance via multiple dedicated officers was no longer required because new devices "make long-term monitoring relatively easy and cheap."[96] In the past, important investigations used a wide array of technologies. Now, one device can reveal the same information, such as singular

---

an individual does not receive Fourth Amendment protection in an unoccupied or undeveloped area outside of the curtilage of one's home). *But see* Benjamin M. Ostrander, *The "Mosaic Theory" and Fourth Amendment Law*, 86 NOTRE DAME L. REV. 1733, 1746–47 (2011) (noting that in *Knotts*, though the electronic beeper surveillance spanned over one day, "it was practically impossible for an individual to observe the whole of the defendant's interstate movements").

86. *See Maynard*, 615 F.3d at 559–60.

87. *See id.* at 559 ("[W]e ask not what another person can physically and may lawfully do but rather what a reasonable person expects another might actually do.").

88. *See* Kerr, *supra* note 28, at 324.

89. *See Maynard*, 615 F.3d at 561–63.

90. *See id.* at 562.

91. *See id.* at 558; *see also* U.S. Dep't of Just. v. Reps. Comm. For Freedom of Press, 489 U.S. 749, 763–64 (1989) (holding that disclosure of the contents of Federal Bureau of Investigation (FBI) criminal identification records to a third party may reasonably be an unwarranted invasion of personal privacy).

92. *See Maynard*, 615 F.3d at 563.

93. *See* United States v. Jones, 565 U.S. 400, 431 (2012) (Alito, J., dissenting); *Maynard*, 615 F.3d at 558.

94. *See Jones*, 565 U.S. at 431.

95. *See id.* at 425, 429.

96. *Id.* at 428–29.

GPS tracker.[97] Justice Alito suggested that the *use* of the GPS tracker was a search because the information was collected over a "lengthy" period and consequently broke societal expectations of privacy.[98]

Like Justice Alito, Justice Sotomayor eschewed the theory of search based on the installation and opted for the *Katz* test to account for surveillance methods that do not require trespass.[99] Justice Sotomayor argued that the GPS tracker's "unique attributes," including precision, comprehension, and ease of adoption and use, should be considered independent of time.[100] She proposed that courts should consider these attributes to determine whether an expectation of privacy exists "in the sum of one's public movements."[101] The government may determine a person's beliefs and habits by a viable reasonableness standard as set by societal expectations of their movements being "recorded and aggregated."[102] Though Justice Sotomayor starts the inquiry at the surveillance tool's unique characteristics, she argues that reasonableness depends on the revealing nature of the "intimate information" even where aggregated through "mundane tasks."[103]

The Court has repeatedly turned to whether the search was reasonable by reviewing the privacy interests despite the Court's grounding in a trespass-like standard and its multiple reaffirmations.[104] This historical trend may be because a person's privacy, within the context of a government search, is deeply rooted in the Constitution.[105] With *Katz* as the trend's "lodestar," the Court has attempted to reconcile Fourth Amendment rights with the advancement of new technologies.[106] Consequently, the mosaic theory has sporadically sprung up to

97. *See id.* (referencing, in Justice Alito's concurrence, the progression of investigation techniques from cell towers to "phone-location-tracking-services").

98. *See id.* at 430–31.

99. *See id.* at 414–15 (Sotomayor, J., dissenting) ("[C]ourts have recognized longstanding protection for privacy expectations inherent in items of property that people possess or control.").

100. *Id.* at 415–16.

101. *Id.* at 416.

102. *Id.* (Justice Sotomayor then drew the natural corollary that considered the potential harm from law enforcement's misuse of the surveillance tool).

103. *See id.* at 416–18.

104. *See, e.g.*, *id.* at 414, 425; United States v. Karo, 468 U.S. 705, 716–17 (1984); Kyllo v. United States, 533 U.S. 27, 31–33 (2001); United States v. Miller, 425 U.S. 435, 442 (1976); Smith v. Maryland, 442 U.S. 735, 739–40 (1979); Katz v. United States, 389 U.S. 347, 361 (1967) (Harland, J., concurring). *But see, e.g.*, Silverman v. United States, 365 U.S. 505, 509 (1961); On Lee v. United States, 343 U.S. 747, 754–55 (1952); Goldman v. United States, 316 U.S. 129, 134–35 (1942), *overruled by* Katz v. United States, 389 U.S. 347 (1967); Olmstead v. United States, 277 U.S. 438, 466 (1928); Boyd v. United States, 116 U.S. 616, 630 (1886).

105. *See* Dobbs v. Jackson Women's Health Org., 142 S. Ct. 2228, 2351 n.48 (2022) (citing *Katz*, 389 U.S. at 351, 353 (recognizing that the Fourth Amendment extends to material and communications that a person "seeks to preserve as private," and rejecting the more limited construction articulated in *Olmstead*, 277 U.S. at 438.)).

106. *Smith*, 442 U.S. at 739. *Compare* Peter P. Swire, *Katz Is Dead. Long Live Katz.*, 102 MICH. L. REV. 904, 905 (2004) ("[The] Fourth Amendment doctrine should continue to play a role in governing electronic surveillance and other high-tech searches."), *with* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 805 (2004) (arguing against "an aggressive judicial role in the application of the Fourth Amendment to new technologies").

resolve the issue of the reasonableness of societal expectations for new and existing surveillance tools.[107]

B. THE SEISMIC SHIFT OF THE PRIVACY STANDARD AND ITS AFTERSHOCKS

In 1967, the Supreme Court upended the traditional trespassory test by holding in *Katz v. United States* that "the Fourth Amendment protects people, not places."[108] Many of the Court's previous inquiries centered on whether the search occurred within a "constitutionally protected area."[109] Suddenly, the Court sought a test based on a reasonable expectation of privacy.[110] Where *Katz* sought to preserve "individual privacy," the third-party doctrine emerged as its counterbalance.[111] Under the third-party doctrine, a person cannot claim to have a reasonable expectation of privacy if they voluntarily hand information over to a third party.[112] A warrant might not be required to collect information from third parties in everyday behaviors such as dialed phoned numbers for calls and text messages from cell service providers, websites ("URLs") and email addresses from internet service providers, and groceries and medications from online retailers.[113]

Under the STP, the San Francisco Police Department collects videos, images, date and time, and geolocation data, which may reveal more than a recorded individual intended through their everyday behaviors.[114] To forecast how courts may assess the constitutionality of the STP as well as pole cameras, I provide several cases that illustrate how the Fourth Amendment pendulum has swung between a pure application of the reasonable expectation of privacy test and the third-party doctrine for the past half-century.[115]

1. Katz v. United States*: Eavesdropping Device*

In *Katz*, government agents affixed a microphone to the outside of a public phone booth without a warrant, then recorded Charles Katz's conversations before charging him with transmitting wagering information in violation of a federal statute.[116] In recognition of shifting societal norms and technologies, the

107. *See, e.g.*, United States v. Jones, 625 F.3d 766, 769 (D.C. Cir. 2010) (Sentelle, C.J., dissenting) ("I cannot discern any distinction between the supposed invasion by aggregation of data between the GPS-augmented surveillance and a purely visual surveillance of substantial length.").

108. *Katz*, 389 U.S. at 351.

109. *See, e.g.*, Lanza v. New York, 370 U.S. 139, 143 (1962) (jails); Rios v. United States, 364 U.S. 253, 261 (1960) (taxicabs); Henry v. United States, 361 U.S. 98, 103–04 (automobiles); Lustig v. United States, 338 U.S. 74, 78–79 (1949) (hotel rooms); Amos v. United States, 255 U.S. 313, 314 (1921) (stores); Silverthorne Lumber Co. v. United States, 251 U.S. 385, 390 (1920) (business offices).

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

111. *See id.* at 350; Tonja Jacobi & Dustin Stonecipher, *A Solution for the Third-Party Doctrine in A Time of Data Sharing, Contact Tracing, and Mass Surveillance*, 97 NOTRE DAME L. REV. 823, 825 (2022).

112. *See* Jacobi & Stonecipher, *supra* note 111, at 825.

113. *See Jones*, 565 U.S. at 417.

114. Non-City STP, *supra* note 15, at 5.

115. *See* Kerr, *supra* note 44, at 519.

116. *Katz*, 389 U.S. at 348.

Supreme Court extended Fourth Amendment protection against warrantless electronic eavesdropping for conversations outside a traditional constitutionally protected area.[117] The Court held "what [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[118] The Government's monitoring constituted a search because Katz expected that his conversation would "not be broadcast to the world" once he shut the booth's door.[119]

Justice Harlan's concurrence in *Katz* created the two-prong test to determine if a search occurred: First, whether a person "exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[120] Reasonableness primarily rests on the information sought, not the surveillance method used to acquire such information, because law enforcement may use technologies in ways unforeseen by the public. This is a pressing concern with regards to new and developing technologies.[121]

The judicial designation of government conduct as a "search" determines the limits of law enforcement's warrantless investigation tools and methods.[122] Government actions that do not amount to a search do not require a warrant under the Fourth Amendment.[123] However, the Supreme Court raised the threshold of acceptable warrantless surveillance by holding what a person "knowingly exposes to the public . . . is not the subject of Fourth Amendment protection."[124] The "knowingly exposes" exception served as the basis for the third-party doctrine, in which a mere presumption of knowledge should not eliminate constitutional protections.[125] However, the first two post-*Katz* cases that involved warrantless information sharing shaped the third-party doctrine by

117. *See id.* at 351–353 ("To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication."); Kerr, *Equilibrium-Adjustment Theory*, *supra* note 44, at 515 ("[T]he power to monitor communications in a phone booth when a person placed a call was the modern equivalent to the power to break into a home and listen to conversations there.").

118. *Katz*, 389 U.S. at 351–52.

119. *Id.* at 352.

120. *Id.* at 361.

121. *See* Ric Simmons, *From* Katz *to* Kyllo*: A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technologies*, 53 HASTINGS L.J. 1303, 1304, 1312 (2002). *Cf.* Orin S. Kerr, Katz *Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. CHI. L. REV. 113, 133–34 (2015) (arguing that *Katz*'s subjective prong is a phantom doctrine because it is rarely applied or has little to no impact on the outcomes).

122. Kerr, *supra* note 28, at 94.

123. *See id.*

124. *See Katz*, 389 U.S. at 351; *see also* California v. Ciraolo, 476 U.S. 207, 213–14 (1986) (holding that aerial observation of a fenced backyard without a warrant did not violate a person's Fourth Amendment rights because the defendant knowingly exposed his backyard to the unaided view of "[a]ny member of the public flying in this airspace").

125. *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979) ("[A] person has no legitimate expectation of privacy in information [they] voluntarily turn[] over to third parties."); United States v. Miller, 425 U.S. 435, 443 (1976) ("[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authority authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence place in the third party will not be betrayed."); *Katz*, 389 U.S. at 351.

creating a per se rule under the presumption of knowledge as opposed to following the existing two-prong test.[126]

2. United States v. Miller*: Bank Records (Defective Subpoena)*

In *United States v. Miller*, the Government obtained the financial bank account records of Mitch Miller because federal agents discovered illegal whiskey distilling equipment on his property through a defective subpoena.[127] Faced with tax evasion charges, Miller challenged the admissibility of the bank records by citing the prohibition against the compulsory production of private papers in *Boyd*.[128] Miller argued that the combination of the bank's recordkeeping and subpoena amounted to an end run around the Fourth Amendment.[129] The Supreme Court was unconvinced, holding that the records were the property of the bank and depositors had adequate protection from improper government access to their records by the "existing legal process."[130] Since banks are required to keep records and banks operate as third-party mediums for transactions, the Court held that Miller had no reasonable expectation of privacy in the documents that "contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."[131] The Court reasoned that the bank customer assumes the risk that the third-party bankers would convey financial and other information to the Government.[132] Unlike *Katz* where the defendant chose to use the public phone booth, *Miller* reduced the "knowingly exposes" exception to constitutional protection to passive conduct despite the lack of options in handing over financial information when interacting with the bank, and thereby created the third-party doctrine.[133]

3. Smith v. Maryland*: Pen Register*

Smith v. Maryland similarly removed the voluntariness requirement and subsequently expanded the third-party doctrine to include the phone numbers dialed from home telephones.[134] In *Smith*, police officers asked—without a warrant—a phone company to install a pen register in its offices to record the phone numbers dialed from the home phone of Michael Smith, who was suspected of robbery and harassment.[135] After the phone company complied and

126. *See Miller*, 425 U.S. at 436; *Smith*, 442 U.S. at 745–46; Jacobi & Stonecipher, *supra* note 111, at 834.
127. *Miller*, 425 U.S. at 436–37.
128. *Id.* at 436, 439.
129. *Id.* at 441.
130. *Id.* at 439, 440 (internal citations omitted).
131. 12 U.S.C. § 1829b(b) (1976) (amended 2004); *Miller*, 425 U.S. at 440, 442.
132. *Miller*, 425 U.S. at 443.
133. *See* Jacobi & Stonecipher, *supra* note 111, at 875–76.
134. *See id.*; *see also* Michael Gentithes, *The End of* Miller*'s Time: How Sensitivity Can Categorize Third-Party Data After* Carpenter, 53 GA. L. REV. 1039, 1053–58 (2019).
135. *Smith*, 442 U.S. at 737.

Smith was indicted,[136] Smith invoked *Katz* and argued that the installation and use of the "pen register's limited capabilities" intruded upon his protected privacy.[137] Yet, the Supreme Court distinguished pen registers as devices that "do not acquire the *contents* of communications" and less offensive than divulging what the caller or recipient said, their identities, and whether the connection was successful.[138] The Court held that the use of the pen register was not a search because Smith had no reasonable expectation of privacy in the dialed numbers or their disclosure to the phone company, which operated as a third party, like the banks in *Miller*, to facilitate conversations between persons.[139]

The basic nature of the collected information led the Court to assume that phone users knew that their dialed numbers were transmitted to the phone companies to route their calls and that the numbers were recorded for billing purposes.[140] The Court misapplied *Katz*'s subjective prong because justices may only speculate on another person's subjective belief whereas only the individual in question may state what they truly believed.[141] The Court concocted a reasonable person to serve as a proxy to Smith, then it deemed neither prong of *Katz* as satisfied.[142] Thus, the installation and use of the pen register did not require a warrant.[143]

Justice Marshall raised two fundamental flaws in the majority's reasoning.[144] He argued that Smith lacked meaningful choice because society deemed the home phone to be "a personal or professional necessity" without a realistic alternative.[145] Justice Marshall also argued that "to make risk analysis dispositive in assessing the reasonableness of privacy expectations would allow the government to define the scope of Fourth Amendment protections."[146] He believed that the government would avoid the boundaries of the Fourth Amendment by announcing its intent to monitor conversations or documents, thereby putting individuals on notice.[147] For cases that implicate information conveyed to the government by third parties, Justice Marshall proposed that the analysis factors in the risks that one is "forced to assume in a free and open society."[148]

136. *Id.*
137. *Id.* at 737, 741–42.
138. *Id.* at 741.
139. *Id.* at 742.
140. *Id.* at 743–45.
141. *See* 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE § 2.1(c) (6th ed. 2020).
142. *See Smith*, 442 U.S. at 742–46.
143. *Id.* at 745–46.
144. *Id.* at 749 (Marshall, J., dissenting).
145. *Id.* at 750.
146. *Id.*
147. *Id.*
148. *Id.*

For transactions involving exposed information, *Katz*, *Miller*, and *Smith* struck at different elements of privacy, including its purpose, amount, and recipients, that form a person's privacy expectations.[149] For analyzing the purpose of transactions, the government seeks information, such as one's address, to tax, prosecute, and mail ballots for elections. On the other hand, private persons may seek to instantaneously communicate by phone, facilitate financial transactions, or engage in idle gossip, but their intended exposure of information is limited to those goals.[150] Regarding the amount of information exposed, the government with its vast resources may collect far more data than what a person reveals to their friend, bank teller, or even an online merchant.[151] Despite a lengthy recitation of one's activity over the course of a day, a person reasonably expects the third party to not retain all information in near perpetuity. Further, a person generally provides information to third parties in "small, discrete parts" with the reasonable expectation that the entirety of the day's events is not compiled.[152] For example, a person may ask a post office clerk to temporarily hold mail until returning from vacation, display their badge to the security guard to enter their workplace, and tap their credit card at a grocery store before heading home, but does not necessarily expect each third party to have information voluntarily disclosed to other parties. Finally, the difference in recipients dictates their use of the same information. [153] For example, the address conveyed to an online retailer may be used as a mailing address for packages as opposed to the same address that is communicated to a registrar of voters as a residential address for an upcoming election. On the other hand, when the government seeks exposed information, it may be for evidence gathering.[154]

Since *Smith* significantly increased the burden of defendants to show that government action constituted an unreasonable search, the below Supreme Court cases demonstrate attempts to restore equilibrium as law enforcement used new technologies in their investigations.[155]

4. United States v. Karo*: Electronic Beeper*

In *United States v. Karo*,[156] federal agents learned from an informant that James Karo and other defendants ordered ether to extract cocaine from imported

149. *See* John S. Applegate & Amy Applegate, *Pen Registers After* Smith v. Maryland, 15 HARV. C.R.-C.L. L. REV. 753, 758 (1980).

150. *Id.*

151. *See* United States v. Jones, 565 U.S. 400, 415–16 (2012) (Sotomayor, J., concurring).

152. *See* Applegate & Applegate, *supra* note 149, at 758.

153. *See id.*

154. *See id.*

155. *See* Kyllo v. United States, 533 U.S. 27, 34 (2001); United States v. Karo, 468 U.S. 705, 716 (1984); Kerr, *supra* note 44, at 480, 499–500, 533–34.

156. *Cf.* United States v. Knotts, 460 U.S. 276, 277–80 (1983) (holding that surveillance did not invade the cabin owner's expectation of privacy and that the beeper's use was not a search where narcotics agents attached a beeper to a chloroform container, the beeper remained in a car travelling mainly on public streets and highways, and agents did not monitor it inside the cabin).

clothing and subsequently obtained a court order authorizing the installation and monitoring of a beeper in a can of ether.[157] The agents swapped the cans,[158] saw Karo retrieve the beeper can, followed him to his house, and used the beeper to determine that the ether was inside the house and continued monitoring its location.[159] The ether was moved in succession to two other houses, lockers in two commercial storage facilities, another defendant's house, and a house rented by multiple defendants.[160] Again, the agents determined that the beeper was inside the house, then obtained a warrant to arrest the defendants and seize the cocaine.[161]

The Supreme Court held that the Government's use of the beeper to monitor the can's location in the *home* violated the defendants' Fourth Amendment rights.[162] The Court reasoned that the monitoring by beeper "reveal[ed] a critical fact about the interior of the premises that the Government is extremely interested in knowing and that it could not have otherwise obtained without a warrant."[163]

The Court was not persuaded by the Government's difficulty in meeting the particularity requirement to secure a warrant, but it outlined the elements needed for the issuance of a warrant.[164] Further, the Court held that the warrant procedure necessarily "interpose[d] a 'neutral and detached magistrate' between the citizen and the 'the officer engaged in the often competitive enterprise of ferreting out crime.'"[165] Thus, where *Knotts* concerned the Government tracking a person's movements in public, *Karo* maintained that a person still has a reasonable expectation of privacy of their location at their home whether present or not. However, the conundrum is that beepers and other devices that are used to monitor one's movements will inevitably lead to tracking a person in both public and private places.

5. Kyllo v. United States*: Thermal Imager*

Like *Karo*, *Kyllo v. United States* limited *Knotts*'s holding to the public sphere.[166] Federal agents suspected Danny Kyllo of using his home to grow

157. *Karo*, 468 U.S. at 708.

158. *See id.* (noting that the informant consented to replacing one of the original cans of ether with the tracked can).

159. *Id.*

160. *Id.* at 708–10 (acknowledging that other circumstances, including the visual monitoring throughout transit and the beeper's lack of precision for which locker contained the ether, provided sufficient untainted evidence to issue the subsequent warrant).

161. *Id.* at 710.

162. *Id.* at 714, 718.

163. *Id.* at 715.

164. *Id.* at 718 (noting that, where it may be impossible to describe a place to be searched, a warrant may be issued if the government describes the beeper's concealing object, the circumstances leading to use, and its requested duration of surveillance).

165. *Id.* at 717 (quoting Johnson v. United States, 333 U.S. 10, 14 (1948)).

166. *Cf.* United States v. Knotts, 460 U.S. 276, 284–85 (1983) (holding that technological advancements that "enable[] the police to be more effective in detecting crime" do not "equate[] . . . with unconstitutionality").

marijuana.[167] After obtaining a subpoena for Kyllo's utility records, the agents discovered that Kyllo's electricity use was abnormally high. The agents used a thermal imager to detect whether the heat images of Kyllo's home were consistent with indoor marijuana cultivation that used high-intensity lamps.[168] The agents completed the scan in a few minutes from across the street.[169] The scan revealed that the roof over Kyllo's garage was "substantially warmer than neighboring homes."[170] Based on the informant's tip, utility bills, and the scan, the agents obtained and executed a warrant to search Kyllo's home, where they found an indoor marijuana growing operation.[171] Despite the absence of physical intrusion into the defendant's home, the Supreme Court held that the use of "sense-enhancing" thermal imaging was a Fourth Amendment search because the technology allowed the Government to obtain "details of the home that previously have been unknowable without physical intrusion." The intrusive search of intimate details of Kyllo's home was thus unreasonable.[172]

The Court rejected the Government's argument that only heat *from* the walls as opposed to *through* the walls was observed because it was sensitive to "leav[ing] the homeowner at the mercy of advancing technology."[173] Further, the Court noted that "[i]t would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology."[174] However, the Court was keen to limit its holding to devices that are "not in general public use."[175] Therefore, the Court indicated that a person's reasonable expectation of privacy is inversely correlated with a technology's adoption rate or use in society.[176]

The issue that remained after *Kyllo* was whether its holding would be flexible enough to lend itself to the third-party doctrine for future technologies or older technologies reinvented with new features, like pole cameras, in the public.[177] However, Fourth Amendment protections need not rely on *Kyllo* alone

167. Kyllo v. United States, 533 U.S. 27, 29 (2001).

168. *Id.* at 29–30 ("Thermal imagers detect infrared radiation, which virtually all objects emit but which is not visible to the naked eye. The imager converts radiation into images based on relative warmth—black is cool, white is hot, shades of gray connote relative differences; in that respect, it operates somewhat like a video camera showing heat images.").

169. *Id.* at 30.

170. *Id.*

171. *Id.*

172. *Id.* at 34, 40.

173. *Id.* at 35–36.

174. *Id.* at 33–34.

175. *See id.* at 40; *see also* Florida v. Jardines, 569 U.S. 1, 11 (2013) ("[W]hen the government uses a physical intrusion to explore details of the home (including its curtilage), the antiquity of the tools that they bring along is irrelevant.").

176. *Cf. Kyllo*, 533 U.S. at 34 (noting that "[t]he *Katz* test . . . has often been criticized as circular" because, as one's reasonable expectation of privacy decreases, the type of government intrusions that are not Fourth Amendment searches increases; *Katz* is thus rendered ineffective at protecting privacy).

177. Security cameras now benefit from high resolution and function in low light. They can be outfitted with sensors that detect specific audio sounds, identify motion, temperature, and humidity changes; some video

because the Supreme Court curtailed the third-party doctrine for the digital age, albeit returning no less than three separate dissents.[178]

C. THE THIRD-PARTY DAMPER

Unlike many of the seminal cases involving law enforcement's investigation techniques and tools, *Carpenter v. United States* involved a federal statute.[179] The Stored Communications Act ("SCA") governs "stored wire and electronic communications and transactional records" held by third-party network service providers.[180] The crux of the SCA (and *Carpenter*) is 18 U.S.C. § 2703, which dictates the procedures that law enforcement must follow to compel third parties to disclose user data.[181] The statute simultaneously grants the Government authority to acquire a person's data from a third party, which falls outside of constitutional protection, and a person the right to restrict access to certain categories of digital information, especially content data.[182]

Congress assigned different levels of protection based on the type of information disclosed and the number of days held in electronic storage for unopened content, such as uncollected email, or transitory email that sits on the internet service provider's server.[183] Generally, the SCA requires a search warrant, including probable cause, for the content of emails, including the body text of messages, but a subpoena is sufficient for basic subscriber information, session logs, and internet protocol ("IP") addresses.[184]

---

surveillance systems can process data with artificial intelligence and databases. Stanislava Ilic-Godfrey, *Artificial intelligence: taking on a bigger role in our future security,* U.S. BUREAU LAB. STAT., BEYOND NOS., (May 3, 2021), https://www.bls.gov/opub/btn/volume-10/investigation-and-security-services.htm.

178. *See* Carpenter v. United States, 138 S. Ct. 2206, 2216–17, 2219–22 (2018).

179. *Id.* at 2221; 18 U.S.C. §§ 2701–12 (2018) (originally enacted as Title II of the Electronic Communications Privacy Act of 1986, ch. 121, §§ 2701–10, 100 Stat. 1860 (codified as amended in scattered sections of 18 U.S.C.)).

180. 18 U.S.C. §§ 2510(15), 2711(2) (2021); JIMMY BALSER, COG. RSCH. SERV., LSB10801, OVERVIEW OF GOVERNMENTAL ACTION UNDER THE STORED COMMUNICATIONS ACT (SCA) 2 (2022) (clarifying that providers consists of electronic communication services providers, such as cell phone providers, email providers, and social media platforms, and remote computing service providers, such as cloud computing providers). *But see* Eric R. Hinz, Note, *A Distinctionless Distinction: Why the RCS/ECS Distinction in the Stored Communications Act Does Not Work*, 88 NOTRE DAME L. REV. 489, 514–18 (2012). *See generally* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (2004) (explaining the mechanics of the statute).

181. 18 U.S.C. § 2703 (2018).

182. Alan Z. Rozenshtein, *Fourth Amendment Reasonableness After* Carpenter, 128 YALE L.J.F. 943, 944 (2019).

183. 18 U.S.C. §§ 2702–03 (2018); Kerr, *supra* note 180, at 1222–24. *But see* 1 WAYNE R. LAFAVE, JEROLD H. ISRAEL, NANCY J. KING & ORIN S. KERR, CRIMINAL PROCEDURE § 4.4(c) (4th ed. 2022) (noting that in some circuits, time may no longer differentiate the type of request that law enforcement must make to compel disclosure because in *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010), the court held that the government must secure a warrant to obtain the content of an email regardless of time).

184. *See* 18 U.S.C. § 2703(c) (2018); Kerr, *supra* note 180, at 1222–24.

1. Carpenter v. United States*: Cell-Site Location Information*

In 2018, the government suspected Timothy Carpenter of a string of robberies, so it obtained section 2703(d) orders, which required particular facts that showed the "reasonable grounds" and "relevancy" of the information sought, for cell-site location information ("CSLI").[185] The first and second orders provided 127 and 2 days of CSLI records, respectively, and cataloged an average of 101 data points per day.[186] The Government used the CSLI to place Carpenter at the scene of each robbery and subsequently charged Carpenter.[187] Carpenter moved to suppress the evidence, which he claimed required a warrant and probable cause rather than a section 2703(d) order.[188]

The Supreme Court held that the compelled disclosure of historical CSLI that provides "a comprehensive chronicle of the user's past movements" is an unreasonable search.[189] Further, the Government must obtain a warrant to acquire seven or more days of historical CSLI.[190] Writing for the majority, Chief Justice Roberts acknowledged the tension between a person's reasonable expectation of privacy and the third-party doctrine, then sequentially analyzed the facts under the privacy test and its exception while nodding to the mosaic theory.[191]

First, the Court found that Carpenter's expectation of privacy in his movements was reasonable because, like GPS tracking in *Jones*, CSLI is "detailed, encyclopedic, and effortlessly compiled."[192] The "all-encompassing record" of a person's location, with an accuracy ranging from "one-eighth to four square miles," sufficiently described Carpenter's location such that the Government emphasized it at Carpenter's trial.[193] "[T]ime-stamped data provides an intimate window into a person's life," which may reveal more than mere movements.[194] The Court noticed the lack of constitutional and practical safeguards because law enforcement could readily request and use CSLI.[195]

---

185. 18 U.S.C. § 2703(d) (2018); Carpenter v. United States, 138 S. Ct. 2206, 2211–12 (2018) (noting that cell service providers use CSLI, which is generated when a phone connects to a cell site, to route data efficiently based on the nearest cell site, improve network coverage, and apply roaming fees).

186. *Carpenter*, 138 S. Ct. at 2212.

187. *Id.* at 2211–13.

188. *Id.* at 2212.

189. *Id.* at 2211, 2224.

190. *Id.* at 2217 n.3 ("It is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search.").

191. *See id.* at 2214–16 ("[R]equests for cell-site records lie at the intersection of two cases, both of which inform our understanding of the privacy interests at stake."); Bert-Jaap Koops, Bryce Clayton Newell & Ivan Škorvánek, *Location Tracking by Police: The Regulation of "Tireless and Absolute Surveillance*,*"* 9 UC IRVINE L. REV. 635, 693 (2019).

192. *Carpenter*, 138 S. Ct. at 2216.

193. *Id.* at 2217–18.

194. *Id.* at 2217 (quoting United States v. Jones, 565 U.S. 400, 415 (Sotomayor, J., concurring)) ("[T]hrough [movements] his 'familial, political, professional, religious, and sexual associations'" are revealed.). *Cf.* United States v. Knotts, 460 U.S. 276, 284 (holding that because a beeper has rudimentary tracking and not sweeping surveillance capabilities, little information can be revealed by the device alone).

195. *Id.* at 2217–18.

Next, the Court rejected the Government's argument that CSLI falls within the third-party exception due to its "unique nature."[196] By pointing to the limited information that may be revealed to third parties, the Court suggested a device's primary purpose and the breadth of detailed information exposed curtail the third-party doctrine.[197] The Court also indicated that voluntariness of exposure depends on the lack of meaningful choice to function in contemporary society.[198]

In a scathing dissent, Justice Kennedy accused the majority of creating a balancing test in which the privacy interests of "each 'qualitatively different category' of information" must be weighed against the extent of their disclosure to a third party.[199] The administrability of the balancing standard may be untenable in the digital age, where electronic information is plentiful.[200] Justice Kennedy also criticized the majority for the arbitrariness of the inferred line of permissible days before the warrantless request constitutes an unreasonable search.[201]

However, the separate dissents of Justices Thomas and Gorsuch hint at the possible future of Fourth Amendment inquiries. Justice Thomas noted that a draft of the Fourth Amendment "changed 'other property' to 'effects'," which may have "broadened the Fourth Amendment by clarifying that it protects commercial goods, not just personal possession."[202] Moreover, in the information age, data has commercial value, hence the prevalence of data mining as an industry.[203] Justice Gorsuch bluntly stated that Carpenter "did not invoke the law of property or any analogies to the common law . . . I cannot help, but conclude—reluctantly—that Mr. Carpenter forfeited his more promising line of argument."[204] Without "disturb[ing] the application of *Smith* and *Miller*," Justices Thomas and Gorsuch suggested that a person may have a nontrivial property interest even in the data held by a third party under the Fourth Amendment itself.[205] Further, Justice Gorsuch implied that a person may have standing in positive law rights, such as the right to be forgotten, conferred by data privacy statutes.[206]

196. *Id.* at 2219–20.

197. *See* Riley v. California, 573 U.S. 373, 393–96 (2014) (holding that a warrant is required to search and seize cell phone data because of the combination of their "immense storage capacity" and multiple functions beyond telephony allow law enforcement to "reconstruct someone's specific movements" and discover "all aspects of a person's life"); Smith v. Maryland, 442 U.S. 735, 742 (1979); United States v. Miller, 425 U.S. 435, 442 (1976).

198. *See Carpenter*, 138 S. Ct. at 2220.

199. *See id.* at 2231–32 (Kennedy, J., dissenting).

200. *See Riley*, 573 U.S. at 394.

201. *See Carpenter*, 138 S. Ct. at 2233–34 (holding that seven days of CSLI records corresponds to the government's § 2703(d) request and the two days of CSLI records provided does not).

202. *Id.* at 2241.

203. *See* Sorrell v. IMS Health Inc., 564 U.S. 552, 558 (2011) (recognizing that prescriber-identifying information has commercial value, especially for drug manufacturers, consultants, and pharmacies).

204. *Carpenter*, 138 S. Ct. at 2272.

205. *See id.*

206. *See id.* at 2220, 2272.

Though the Court attempted to restrict *Carpenter*'s holding to historical CSLI, its rule is far-reaching.[207] The Court recognized that new technology was increasing the accuracy of CSLI, thereby calling into question the decisions based on technologies that the Court has previously ruled on that have since advanced.[208] If more precise or detailed information can be exposed, then the third-party doctrine may not apply. Although the Court upheld the validity of "security cameras," it left the door open for pole cameras and other surveillance systems whose technological capabilities may exceed "conventional surveillance techniques and tools" due to the breadth, depth, and ease of data collection as well as the nature of videos themselves.[209]

II. PERVERSE POLE CAMERAS POINT IN TWO DIRECTIONS

In response to a rise in crime, the San Francisco Board of Supervisors passed an ordinance and modified their STP.[210] The revised STP created a network of surveillance cameras through a partnership agreement with the camera's owner, and not the device's manufacturer or software service provider, like Amazon's Ring.[211]

A cryptocurrency mogul's four-million-dollar spending spree created a de facto network with over 1,000 cameras purchased.[212] The camera system uses advanced video and evidence management, and it has the potential for license plate reading and facial recognition.[213] San Francisco's residents and business owners may place the cameras on private property. [214] Each neighborhood coalition, but not every property owner, controls access to the live feed or historical footage, which includes granting access to SFPD.[215] The cameras are

207. *See id.* at 2220 ("Our decision today is a narrow one. We do not express a view on matters not before us: real-time CSLI . . . . We do not . . . call into question conventional surveillance techniques and tools, such as security cameras. Nor do we address other business records that might incidentally reveal location information."); *see also* Rozenshtein, *supra* note 182, at 944 ("[E]ven if congressionally authorized, any process short of obtaining a warrant—and thus any level of suspicion less than probable cause—would be unconstitutional."). *But see* Jordan M. Blanke, Carpenter v. United States *Begs for Action*, U. ILL. L. REV. 260, 260–61 (2018) (noting that the Supreme Court did not overturn the third-party doctrine, but "handed down a narrow decision").

208. *Carpenter*, 138 S. Ct. at 2213–14, 2213 n.1, 2218–19 ("[N]o single rubric definitively resolves which expectations of privacy are entitled to protection. . . . our cases by no means suggest that [a property] interest is 'fundamental' or 'dispositive' in determining which expectations of privacy are legitimate. . . . and we have repeated emphasized that privacy interests do not rise or fall with property rights.") (internal citations omitted).

209. *See id.* at 2216, 2220.

210. Johana Bhuiyan, *Surveillance Shift: San Francisco Pilots Program Allowing Police to Live Monitor Private Security Cameras*, GUARDIAN (Oct. 4, 2022, 6:00 AM EST), https://www.theguardian.com/us-news/2022/oct/04/san-francisco-police-video-surveillance.

211. Non-City STP, *supra* note 15, at 2.

212. *See* Bowles, *supra* note 2.

213. *Id.*

214. *Id.*; *see, e.g.*, Union Square Bus. Improvement Dist. Bd. of Dirs., *Video Surveillance System Usage Policy and Procedures*, at 7 (2019) [hereinafter Union Sq. BID] https://www.documentcloud.org/documents/6770598-USBID-Security-Camera-Program-Policy-Jan20 (uploaded to DocumentCloud by Electronic Frontier Foundation).

215. Union Sq. BID, *supra* note 214.

given to the neighbors for free, and they are always recording.[216] Moreover, SFPD has already taken advantage of the system's convenience to issue mass requests for data and to spy on political protestors.[217] There are few safeguards to prevent the mogul from implementing a policy to mandate the data transfer to law enforcement because he is a private owner of the vast camera network.[218]

Though the Supreme Court has left the validity of surveillance cameras intact, it has not ruled on more invasive variants of the technology with sense-enhancing features or function as part of a dragnet.[219] The Court has also not resolved the validity of prolonged surveillance using pole cameras.[220] However, pole cameras are a useful proxy for the cameras under the STP due to their shared unique attributes.[221] Unlike round-the-clock physical surveillance that may alert a person to a criminal investigation, pole cameras may surreptitiously monitor areas and record movements continuously for extended durations or indefinitely.[222] Further, multiple cameras may be linked to form a comprehensive system that can be monitored from a single control center.[223] These systems combine cameras with different features, such as high resolution, 360-degree field of view, zoom, and thermal imaging, to operate in adverse weather or low light conditions.[224] Likewise, the STP accounts for a variety of cameras and their features.[225] Although SFPD is prohibited from implementing "biometric identification or facial recognition technology," the STP does not prevent private camera owners from using these capabilities and then handing over historical footage to SFPD.[226] When the police have access to the camera

216. *Id.*

217. *See* ELEC. FRONTIER FOUND., *supra* note 9 and accompanying text.

218. *See* Bowles, *supra* note 2 (characterizing the neighborhood coalitions, including Union Square BID, as merely "third-party intermediar[ies]"). *But see* Non-City STP, *supra* note 15, at 2 ("SFPD . . . shall not manage a registry . . . or have a Ring/Neighbors or similar partnership agreements.").

219. *See* Kyllo v. United States, 533 U.S. 27, 34 (2001); United States v. Knotts, 460 U.S. 276, 283–84 (1983); Ilic-Godfrey, *supra* note 177.

220. *Compare* United States v. Moore-Bush, 36 F.4th 320, 331 (1st Cir. 2022) (Barron, C.J., Thompson & Kayatta, JJ., concurring) ("The only cases from the Court to address an even arguably analogous claimed expectation of privacy are *Jones* and *Carpenter*,"), *and id.* at 361 (Lynch, Howard & Gelpí, JJ., concurring) ("*Carpenter* forbids and does not support the [other] concurrence's contention that the use of video taken from the pole camera by the prosecution violated the Fourth Amendment."), *with* United States v. Tuggle, 4 F.4th 505, 510–11 (7th Cir. 2021) (noting this case "presents an issue of first impression").

221. *See* United States v. Jones, 565 U.S. 400, 415–16 (2012).

222. *See* MCKENNA & FISHMAN, *supra* note 23.

223. NAT'L URB. SEC. TECH. LAB'Y, U.S. DEP'T OF HOMELAND SEC. SCI. & TECH. DIRECTORATE, PUB. NO. SAVER-T-MSR-30, WIRELESS SURVEILLANCE CAMERA SYSTEMS 10–12 (2021), https://www.dhs.gov/sites/default/files/saver_wireless_surveillance_camera_systems_msr_25aug2021-508.pdf.

224. *Id.*

225. Non-City STP, *supra* note 15, at 3–4 (listing examples of cameras, including box cameras, dome cameras, pan-tilt-zoom ("PTZ") cameras, bullet cameras, IP cameras, day-night cameras, wide dynamic cameras, and smart cameras).

226. *Id.* at 2–3.

for live monitoring, the STP lacks any procedures to stop the use of cameras upon discovering that these features remain on.[227]

The STP subverts the role of the neutral and detached magistrate in evidence collection.[228] The STP replaces the subpoena and warrant requirements, which compels the Government to state the facts and circumstances that justify the request for information, with the consent of the private camera owner (absent exigent circumstances).[229] Instead, police officers are only required to provide the date and time of the historical footage requested and whether their requests were approved by a private person.[230] Live monitoring also requires officers to record the captain's approval, duration of access, and whether they were able to access the feed.[231]

The circuit court split on the warrantless, prolonged use of pole cameras, specifically, pan-tilt-zoom ("PTZ") cameras, may shed light on the constitutionality of the STP regarding cameras in fixed, public locations.[232] The split is further complicated by the Supreme Court's denial of certiorari for *United States v. Tuggle* followed by an evenly divided panel of judges in *United States v. Moore-Bush*.[233] In Part II, I examine how the lower courts have interpreted and applied *Carpenter* to surveillance video.

A. *UNITED STATES V. TUGGLE*: THE TUSSLE OVER SEQUENTIAL AND COLLECTIVE INQUIRIES

United States v. Tuggle highlights the difficulties faced by the Seventh Circuit and other courts in drawing a line that determines "whether the warrantless use of pole cameras to observe a home . . . amounts to a [Fourth Amendment] search."[234] The case proves illustrative for surveillance cameras in

227. *See id*; *see also* Dave Maass, *San Francisco Police Nailed for Violating Public Records Laws Regarding Face Recognition and Fusion Center Documents*, ELEC. FRONTIER FOUND. (June 2, 2022), https://www.eff.org/deeplinks/2022/06/san-francisco-police-nailed-violating-public-records-laws-regarding-face (discussing how, after the San Francisco banned government use of facial recognition technology, the San Francisco Police Department circulated an image of a suspect, and the Northern California Regional Intelligence Center used the prohibited technology on the image, and forwarded the results to the Police Department). *But see* Police Presentation, July 11, 2022, *supra* note 6, at 4–6 (referencing AMBER and SILVER alerts); Police Presentation, Sept. 12, 2022, *supra* note 5, at 6–7 (discussing violent offenses).

228. *See* Johnson v. United States, 333 U.S. 10, 13–14 (1948).

229. *See* Non-City STP, *supra* note 15, at 8–9. This Note sets aside extensive discussion of the potential absence of informed consent under the consent-search doctrine for future study. *See generally* Alafair S. Burke, *Consent Searches and Fourth Amendment Reasonableness*, 67 FLA. L. REV. 509 (2015) (describing the development of the consent-search doctrine, which emphasizes the reasonableness of voluntary consent by weighing the governmental and individual interests and is often associated with police coercion tactics).

230. *See* Non-City STP, *supra* note 15, at 8.

231. *Id.*

232. *Compare* United States v. Moore-Bush, 36 F.4th 320, 331 (1st Cir. 2022) (Barron, C.J., Thompson & Kayatta, JJ., concurring), *and id.* at 361 (Lynch, Howard & Gelpí, JJ., concurring), *with* United States v. Tuggle, 4 F.4th 505, 510–11 (7th Cir. 2021).

233. *See Moore-Bush*, 36 F.4th at 331, 361 (Chief Judge Barron is joined by Circuit Judges Thompson and Kayatta and Circuit Judges Lynch, Howard, and Gelpí joined a separate concurrence); Tuggle v. United States, 142 S. Ct. 1107 (2022) (mem.).

234. *See Tuggle*, 4 F.4th at 510, 526–27.

the digital era because the district and appellate courts analyzed the facts through the sequential approach of *Katz* and the collective approach of *Jones* and *Carpenter*.[235]

The Government installed three pole cameras on public property surrounding Travis Tuggle's home because the federal agents found that the neighborhood's seldomly used roads made physical surveillance difficult for the covert investigation. [236] The agents attached two cameras to a telephone pole adjacent to Tuggle's home to monitor the front of his residence and driveway.[237] The agents placed the third camera one block away to surveil a co-defendant's shed, but it could also view Tuggle's home.[238] The agents could remotely operate the cameras to view, pan, tilt, and zoom in real-time, but its remaining feature was limited to a basic lighting system to improve video quality at night.[239] The property had no fence, wall, or other obstruction that would block a passing neighbor.[240] The agents could also review the recordings.[241] For over 18 months, the pole cameras continuously captured approximately 100 instances of Tuggle's suspected methamphetamine transactions with couriers and suppliers.[242] The video evidence provided the basis for a search warrant of Tuggle's residence and his subsequent indictments.[243]

1. District Court: Peeping, Not Prying

Before trial, Tuggle attempted to suppress the evidence by arguing that "the Government violated his reasonable expectation of privacy . . . when it conducted warrantless surveillance of his residence with pole cameras for 18 months."[244] For his motion to suppress, the district court analyzed reasonableness and duration separately.[245] As a preliminary matter, the court dispensed with trespass because the Government did not physically intrude on private property to install or use the cameras.[246]

Under *Katz*, the district court found that Tuggle's interest in the front of his home failed both the subjective and the objective inquiries.[247] For the subjective prong, Tuggle did not attempt to obscure his driveway or the front of his

235. *Id.* at 513, 517.

236. United States v. Tuggle, No. 16-CR-20070, 2018 WL 3631881, at *1 (C.D. Ill. July 31, 2018), *aff'd,* 4 F.4th 505 (7th Cir. 2021).

237. *Id.*

238. *Id.*

239. *Id.*

240. *Id.* at *2.

241. *Id.* at *1–2.

242. *Id.* at *2.

243. United States v. Tuggle, 4 F.4th 505, 512 (7th Cir. 2021).

244. *See* United States v. Tuggle, No. 16-CR-20070, 2019 WL 3915998, at *2 (C.D. Ill. Aug. 19, 2019), *aff'd,* 4 F.4th 505 (7th Cir. 2021) (reviewing the defendant's second motion to suppress as well as his motion to reconsider); *Tuggle*, 2018 WL 3631881, at *2 (reviewing the defendant's initial motion to suppress).

245. *Tuggle*, 2018 WL 3631881, at *2.

246. *Id.* at *3.

247. *Id.*

house.[248] Tuggle's expectation was also not objectively reasonable because "[t]he cameras only captured what would have been visible to any passerby in the neighborhood."[249] Further, the court interpreted *Carpenter* as extending protections "to address surveillance methods implicating new technologies" which did not include "ordinary video cameras that have been around for decades."[250] The district court ruling is unique among post-*Carpenter* judgments in considering whether the type of data is exclusive to the digital age.[251]

Next, the district court found that the eighteen months of monitoring did not transform the Government's use of the pole cameras into a search, but it noted that a longer duration may constitute a search.[252] The court rejected Tuggle's use of prolonged GPS tracking in *Jones* because pole cameras are fixed and cannot "track an individual's movement anywhere in the world."[253]

2. Appellate Court: Rejecting the Mosaic Theory

On appeal to the Seventh Circuit, the defendant presented the issue and his argument under two theories, which the appellate court creatively recast in *United States v. Tuggle*:

> Tuggle first frames the issue as "whether the use of warrantless pole cameras surveillance of Mr. Tuggle's private residence violated his Fourth Amendment rights?"
>
> . . . Tuggle's second theory of a Fourth Amendment violation: that the prolonged and uninterrupted use of those cameras constituted a search. Tuggle characterizes this theory in two ways. First, he argues more generally that the "long-term use of the pole cameras over an extended period of approximately eighteen months violates the Fourth Amendment." Second, he asserts that "[a]pplying the mosaic theory, the use of warrantless pole cameras continuously for over [eighteen] months is unconstitutional under the Fourth Amendment."[254]

The Seventh Circuit separated and analyzed Tuggle's argument not by his two theories advanced, but by the issue literally presented on appeal and his combined theories.[255] Tuggle's first theory indicates that the duration is objectively unreasonable and calls for a sequential review under *Katz* whereas

248. *Id.*
249. *Id.*
250. *Id.*
251. *See* United States v. Tuggle, 2019 WL 3915998, at *1 (C.D. Ill., 2019) (comparing the video to stored data in *Riley*), *aff'd*, United States v. Tuggle, 4 F.4th 505, 512 (7th Cir. 2021), *cert. denied*, 142 S. Ct. 1107 (2022); Matthew Tokson, *The Aftermath of* Carpenter*: An Empirical Study of Fourth Amendment Law, 2018-2021*, 135 HARV. L. REV. 1790, 1828–29 (2022) (analyzing 857 judgments between June 2018 and March 2021 to identify the *Carpenter* factors among lower courts).
252. *Tuggle*, 2018 WL 3631881, at *3.
253. *Id.*
254. United States v. Tuggle, 4 F.4th 505, 513, 517 (7th Cir. 2021) (alterations in original).
255. *See id.*

his second theory calls for a collective review under the mosaic theory.[256] However, the Seventh Circuit mistakenly determined that both theories functionally asked for a review under the mosaic theory.[257] The appellate court's confusion may have arisen from the absence of a mosaic theory discussion at the lower court, which repeatedly rejected the defendant's arguments under the conventional reasonable expectation of privacy framework.[258] Alternatively, the confusion may have stemmed from the complexity in interpreting *Carpenter* and Justices Alito and Sotomayor's concurrences in *Jones* for pole cameras.[259]

First, the Seventh Circuit held that the Government's actions did not constitute a search by applying the sequential framework of *Katz* and omitting duration as a factor entirely.[260] The appellate court concluded that Tuggle did not manifest a subjective expectation of privacy, despite considering it unhelpful.[261] The court also determined that Tuggle's expectation of privacy was unreasonable under the public observation doctrine.[262] The pole cameras were not sense-enhancing tools as in *Kyllo* because the cameras modestly enhanced what a passing neighbor would see, but "they did not do so to a degree that 'give[s] rise to constitutional problems.'"[263] The Seventh Circuit pointed to the Government's limited use of the cameras that only "identif[ied] who visited Tuggle's house and what they carried, all things that a theoretical officer could have observed without a camera."[264]

Second, the Seventh Circuit held that the eighteen months of surveillance did not collectively reveal information that would substantially impact Tuggle's reasonable expectation of privacy.[265] The appellate court presented a brief history of the mosaic theory since *Jones*.[266] The court recognized that "[s]cholars describe the *Carpenter* majority as effectively 'endors[ing] the mosaic theory of privacy,'" but decided not to apply the qualitative analysis that *Carpenter* requires.[267] Rather than weigh on the theory's merits and draw an "arbitrary

256. *See id.* at 513.

257. *See id.* at 517.

258. *See generally Tuggle*, 2018 WL 3631881; United States v. Tuggle, No. 16-CR-20070, 2019 WL 3915998 (C.D. Ill. Aug. 19, 2019), *aff'd,* 4 F.4th 505 (7th Cir. 2021).

259. *See* Dana Khabbaz, *Unmanned Stakeouts: Pole-Camera Surveillance and Privacy After the* Tuggle *Cert Denial*, 132 YALE L.J.F. 105, 116–17 (2022) (summarizing the lower courts' "struggle[] to apply Supreme Court precedent").

260. *See Tuggle*, 4 F.4th at 513.

261. *Id.* at 513–14.

262. *See id.* at 514–15. See also the cases cited *supra* note 84.

263. *See Tuggle*, 4 F.4th at 516 (alteration in original) (quoting Dow Chem. Co. v. United States, 476 U.S. 227, 238 (1986)).

264. *Id.*

265. *Id.* at 517–18.

266. *Id.* at 517–20.

267. *See id.* at 519 (second alteration in original) (quoting Ohm, *supra* note 40, at 373); *see also* Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018) (using the qualitative subtest, which evaluates the *"Carpenter* factors" in the context of mosaic theory, including the information's "deeply revealing nature, . . . depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection.").

line," the Seventh Circuit dismissed Tuggle's argument because it found no "binding caselaw indicating that [it] *must* apply the mosaic theory."[268]

The court pointed to the First, Fourth, Sixth, Ninth, and Tenth Circuits, which "approved the governmental use of cameras" in general.[269] The sole exception was the Fifth Circuit that decided a case involving federal agents' use of a pole camera to record the exterior of the defendant's residence "decades before *Jones* and *Carpenter*."[270] The Seventh Circuit concluded that the defendant's ten-foot-tall fence was the determinative factor that rendered the case inapplicable to Tuggle's home.[271] Absent an overwhelming trend amongst the federal and state courts on whether pole cameras constitute a search, the Seventh Circuit reasoned that duration of use was not dispositive.[272]

Setting duration aside, the Seventh Circuit narrowed the scope of the mosaic theory inquiry to whether the pole cameras "captured the whole of Mr. Tuggle's movements."[273] The court held that the warrantless use of the pole cameras did not constitute a search under the mosaic theory.[274] The court reasoned that, unlike the GPS tracker in *Jones*, the pole cameras were fixed and could not reveal Tuggle's movements beyond his comings and goings near his home.[275] Further, without "an exhaustive record of Tuggle's 'hitherto private routine,'" few intimate details could be revealed.[276]

However, the Seventh Circuit found the breadth of information collected by the pole camera "concerning, even if permissible" because the eighteen-month span was "roughly four and twenty times the duration of the data collection in *Carpenter* and *Jones*, respectively."[277] Despite concluding that no search occurred, the court expressed its "unease about the implications of [pole camera] surveillance for future cases."[278] Further, the Seventh Circuit commented that *Katz*'s two-pronged privacy test warranted reevaluation based on technological growth's "inverse and inimical relationship with individual privacy from government intrusion," which suggested that its hands were bound by precedent.[279] In essence, technological progress lessens the reasonable expectation of privacy. The Supreme Court declined to review the Seventh Circuit's decision.[280]

---

268. *Tuggle*, 4 F.4th at 520, 526.
269. *Id.* at 521.
270. *Id.* at 521–22 (citing United States v. Cuevas-Sanchez, 821 F.2d 248, 251 (1987)).
271. *Id.*
272. *Id.* at 522–23.
273. *Id.* at 523–24 (citing Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018)).
274. *Tuggle*, 4 F.4th at 523–24.
275. *Id.* at 524.
276. *Id.* at 524–25 (quoting United States v. Maynard, 615 F.3d 544, 560 (D.C. Cir. 2010)).
277. *Tuggle*, 4 F.4th at 526.
278. *Id.*
279. *Id. But see Carpenter*, 138 S. Ct. at 2223; United States v. Jones, 565 U.S. 400, 415–16, 424, 428–29 (Alito & Sotomayor, JJ., concurring).
280. Tuggle v. United States, 142 S. Ct. 1107 (2022) (mem.).

B. *UNITED STATES V. MOORE-BUSH*: THE DIFFICULTY IN FOLLOWING *CARPENTER*'S BLUEPRINTS

The Supreme Court's denial of certiorari in *Tuggle v. United States* was anything but final on the constitutionality of the warrantless use of pole cameras.[281] The en banc panel of six judges in *United States v. Moore-Bush* was evenly split on *Carpenter*'s applicability to the case before it, but unanimously reversed the district court's order to grant the defendants' motions to suppress evidence.[282]

Chief Judge Barron and Judges Thompson and Kayatta interpreted the landmark decision as "not limit[ed] to only those situations in which the third-party doctrine is in play," but the judges determined that it applied broadly to the reasonable expectation of privacy test under *Katz*.[283] Consequently, the judges distilled the Supreme Court's purported "embrace [of] something akin to the mosaic theory" to its elements and analogized CSLI data to pole camera videos.[284] Chief Judge Barron and Judges Thompson and Kayatta concluded that the Government "did conduct a Fourth Amendment 'search' when it accessed the digital video record that law enforcement had created over the course of the eight months," so a warrant would be required.[285] However, the judges concluded that the federal agents' actions were exempt "under the 'good faith' exception."[286]

Conversely, Judges Lynch, Howard, and Gelpí interpreted *Carpenter* as "explicitly narrow."[287] The judges reasoned that the Supreme Court's language "did not alter case law surrounding conventional technologies like pole cameras."[288] Further, the defendants' expectation of privacy in their aggregated movements around the residence was unreasonable due to the differences between the CSLI in *Carpenter* and the pole camera videos here.[289] Judges Lynch, Howard, and Gelpí concluded that the Government's actions did not amount to a search, but "law enforcement would have met the probable cause requirement to obtain a warrant."[290] This Note does not cover the good faith exception to the Fourth Amendment's warrant requirement nor the law of the circuit doctrine.[291] Instead, the following section extracts *Carpenter*'s core

281. *Id.*
282. United States v. Moore-Bush, 36 F.4th 320, 320, 361 (1st Cir. 2022) (en banc) (per curiam).
283. *Id.* at 344.
284. *Id.* at 358.
285. *Id.* at 321.
286. *Id.*
287. *Id.*
288. *Id.* at 363.
289. *Id.*
290. *Id.*
291. Under the good faith exception to the search warrant requirement, the exclusion of evidence under the Fourth Amendment is not warranted where a police officer acts in good faith reliance on the warrant issued by the magistrate. *See* Davis v. United States, 564 U.S. 229, 238–41 (2011). Under the law of the circuit doctrine,

meaning and application for pole cameras by reviewing the dichotomy in the First Circuit's interpretation of *Carpenter* to distill its core meaning and application for pole cameras to predict how cases interpreting the San Francisco STP might be argued. Since the appellate court was equally divided, I present both the shared and omitted, pertinent facts from the concurrences.[292]

Before *Carpenter*, federal agents, with cooperation from an undercover informant and state police who seized 921 bags of heroin at a traffic stop, suspected Nia Moore-Bush of arms and drug trafficking at a house that she shared with her mother, a co-defendant.[293] Since the house's location made physical surveillance difficult, federal agents installed a pole camera that provided a twenty-four-seven view of the exposed driveway, garage, and the front of the residence without a warrant.[294] For eight months, the agents monitored the camera's live feed, operated its pan-tilt-zoom feature, and used its recordings to build a collection of images and videos of people's movement, including their license plates and faces through the window of the house.[295] Moore-Bush was arrested and indicted, and, one year after the Supreme Court issued its decision in *Carpenter*, she filed motions to suppress the evidence.[296]

Moore-Bush argued that the Government's prolonged, hidden use of a pole camera was designed to record the activities of everyone associated with the residence and that law enforcement's actions constituted an unreasonable search under the Fourth Amendment.[297] In opposition, the Government argued that the defendant's motions to suppress should be rejected because the police relied, in good faith, on *United States v. Bucci*, which was binding at the time of the monitoring.[298] However, the district court found *Bucci* was not controlling because *Carpenter* invalidated the public observation doctrine.[299] The Government appealed to a panel of judges, which reversed the district court's grant of Moore-Bush's motion to suppress evidence and raised the question of whether *Katz*'s two-prong reasonable expectation of privacy test was correctly applied to *Bucci*; the First Circuit decided to "use this case to give *Bucci* fresh

prior panel decisions by the Court of Appeals remain valid absent a Supreme Court opinion on point, a ruling of the circuit, sitting en banc, or other controlling intervening event, or rarely, where non-controlling but persuasive case law justifies the change. *See* United States v. Chhien, 266 F.3d 1, 11 (2001).

292. *See Moore-Bush*, 36 F.4th at 321–27, 361–63.

293. For the purposes of this discussion, I only reference Nia Moore-Bush and not her mother, who was a co-defendant. *Id.* at 322, 361–62.

294. *Id.* at 323 & n.4, 362.

295. *Id.* at 323, 362.

296. The pole cameras were removed shortly after Moore-Bush's arrest. *Id.* at 324, 362.

297. *Id.* at 324.

298. *Id.* at 326. Judges Lynch, Howard, and Gelpí dispute the other concurrence's disregard for facts and circumstances supporting law enforcement's probable cause because, in their view, *Bucci* and Supreme Court precedent authorized the warrantless use of pole cameras. *See id.* at 322 n.2, 324–25, 363; United States v. Bucci, 582 F.3d 108, 116–17 (1st Cir. 2009) (holding that the use of pole cameras is not a Fourth Amendment search because an individual does not have an expectation of privacy in items or places that they expose to the public).

299. *See* United States v. Moore-Bush, 381 F. Supp. 3d 139, 144–45 (D. Mass. 2019).

consideration en banc."[300] I now address the two concurrences separately for clarity.

1. Search: Building the Foundation for Future Technology

"[T]o ensure that the 'progress of science' does not erode Fourth Amendment protections," Chief Judge Barron and Judges Thompson and Kayatta attempted to modernize the reasonable expectation of privacy framework by permitting Moore-Bush to satisfy each prong of the *Katz* test by its conventional standard or the mosaic theory.[301] The judges concluded that Moore-Bush satisfied both prongs, so a warrantless search occurred and it violated her Fourth Amendment rights.[302]

For the subjective prong, the appellate judges cited the district court's finding that Moore-Bush's "choice of neighborhood and home within it" sufficiently manifested her expectation of privacy, that is to be free from being "surveilled with meticulous precision" over her movements.[303] The Government argued that the defendant failed to take concrete steps, such as erecting a fence or planting a bush, to prevent passing individuals from seeing her in the curtilage of her house.[304] The judges rejected the Government's legal fiction of the "casual, accidental observ[er]" because no bystander could view all activities on the property, and accurately and suddenly recite the "aggregate of activity" from the height of the pole camera.[305] The judges acknowledged that applying the mosaic theory to the aggregate information creates a "compendium," which is a "corollary" of the objective test.[306]

The judges did not define the point at which the defendant's choice to move can no longer transfer to a subjective expectation of privacy.[307] Moore-Bush moved into her mother's house approximately one year before her arrest and the camera pole was installed within three months.[308] When does the timer lapse? For example, compare one's assumptions of a young, wealthy homeowner, who is eager to make upgrades to their property, with an elderly homeowner of twenty-five years, who is saving for retirement. Without elaboration, the judges fell into the same "normative" trap that the *Smith* Court made when imagining a reasonable person within the subjective prong.[309]

300. United States v. Moore-Bush, 36 F.4th 320, 327 (1st Cir. 2022) (en banc) (per curiam).

301. *Id.* at 340.

302. *Id.* at 328.

303. *Id.* at 329 (quoting *Moore-Bush*, 381 F. Supp. 3d at 143).

304. *Id.* at 329.

305. *See id.* at 330; *see also* California v. Ciraolo, 476 U.S. 207, 211–12 (1986) (concerning the expectation of privacy from the aerial observation where few precautions would protect oneself from observation).

306. *See Moore-Bush*, 36 F.4th at 330; *see also* Kerr, *supra* note 121, at 120 (discussing empirical study where no cases were found where the subjective test controlled the outcome).

307. *See Moore-Bush,* 36 F.4th at 322–24.

308. *Id.*

309. *See id.*; Smith v. Maryland, 442 U.S. 735, 742, 745–46.

Several unknown factors cut against tying the subjective prong to property-based principles. For example, one may be a renter that is prohibited from making substantial modifications to the land, thereby they may lack a property interest for standing in cases against the Government. When judges search for manifestations of subjective expectations of privacy, societal norms may unfairly bias the rural farmer, who resides in unprotected, open fields, or the suburban homeowner with fences that block ground-level sight to one's backyard.[310] Alternatively, courts could combine the subjective inquiry with the objective inquiry or skip the subjective prong entirely due to its irrelevance.[311]

Chief Judge Barron and Judges Thompson and Kayatta proceeded to analyze the objective prong and emphasized the inquiry, under the mosaic theory, does not focus on "each discrete activity . . . at the time that it occurred . . . [but] 'the totality of instruments and activities and associations with family members and visitors'" in front of the residence.[312] The judges noted this inquiry necessitated examining at whether the Supreme Court in *Carpenter* used sufficiently similar or broad reasons to allow the First Circuit to extend a person's reasonable expectation of privacy from CSLI to Moore-Bush's movements, activities, and associations.[313] The judges succeeded in analogizing the instant case to *Carpenter* because they connected each *Carpenter* factor to the sacredness of the home.[314]

First, the judges rejected the Government's argument that "what occurred over a lengthy stretch of time at a single locale" did not implicate the same expectation of privacy that should be afforded to the whole of one's movements.[315] Instead, the judges stated that the nature of the place, "the defendants' Hadley Street home," provides deeply revealing information.[316] Further, the judges emphasized that a pole camera exposes information about a person's life such as political, religious, and sexual associations by capturing and recording video, which may be more revealing than mere location tracking.[317]

Second, the judges stated that a person leaving their home would not expect "a perfect form of surveillance to be conducted over a long period of time."[318] By contrasting camera surveillance to tailing, the judges suggested that the Government's monitoring of Moore-Bush had comprehensive reach because "a single-point stakeout" of the defendant's home would capture what she aimed to keep private.[319] Further, the Government "effectively and perfectly captured

310. *See, e.g.*, *Ciraolo*, 476 U.S. at 211–12; Oliver v. United States, 466 U.S. 170, 179 (1984).
311. *See* Kerr, *supra* note 121, at 120.
312. *Moore-Bush*, 36 F.4th at 331–32.
313. *Id.* at 332.
314. *See* Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018).
315. *Moore-Bush*, 36 F.4th at 333.
316. *See id.*
317. *See id.* at 336 (citing *Carpenter*, 138 S. Ct. at 2217) (internal citations omitted).
318. *Moore-Bush*, 36 F.4th at 334.
319. *See id.*

all that visibly occurs in front of a person's home over the course of months," evidencing the breadth of information collected. Despite being only one location, the depth of information revealed was inevitably greater than Moore-Bush's trajectory across the town because that location was her house and curtilage "where privacy expectations are most heightened."[320]

Third, unlike past surveillance efforts that are subject to the "practical limits of manpower and expenses," pole cameras allow the Government to "instantly recall and present for others to observe."[321] Further, the "aggregate of the months of moments" indiscriminately captured relatives, spouses, partners, and friends.[322] Thus, the Government's data collection was automatic and inescapable.

After Chief Judge Barron and Judges Thompson and Kayatta concluded that *Carpenter* extended to the Government's use of the pole camera, they proceeded to address the third-party doctrine.[323] The judges rejected their en banc counterparts' notion that *Carpenter* is "limited to situations in which the third-party doctrine is in play."[324] Instead, the judges interpreted *Carpenter* to be "a 'narrow ruling' that did not apply to 'conventional surveillance techniques.'"[325]

However, they compared the facts here to *Carpenter* again, and determined, for many of the same reasons, the Government's use of the pole camera was not traditional.[326] The sole exception was that the CSLI in *Carpenter* had a "retrospective quality" where the Government could simultaneously view the pole camera's live feed and historical footage.[327] The judges concluded that the Supreme Court's reference to the historical CSLI was inapplicable to Moore-Bush because, in *Carpenter*, the federal agents were limited by "the retention policies of the wireless carriers."[328] Therefore, once the federal agents obtained the CSLI, they gained valuable information that they did not already possess.[329]

Even if a manned stakeout that used the latest digital cameras constitutes a conventional surveillance technique, the judges concluded the Government's "months-long, digital-pole-camera variant" was unusual.[330] Thus, the judges implied that duration is dispositive, apart from digital enhancements.[331]

Critical to the constitutionality of the STP, the judges interpreted *Carpenter*'s reference to "security cameras" to mean "private security cameras

320. *Id.* at 335 (quoting *Ciraolo*, 476 U.S. at 213).
321. *Id.* at 334, 336.
322. *Id.* at 336.
323. *Id.* at 340.
324. *Id.* at 344.
325. *Id.* at 345.
326. *Id.*
327. *Id.* at 347 (citing *Carpenter*, 138 S. Ct. at 2218).
328. *Id.* at 347–48.
329. *Id.* at 348.
330. *Id.* at 352.
331. *See id.* at 339.

guarding private property."[332] The judges cited the amicus curiae brief filed by the National District Attorneys Association, which noted the third-party doctrine's applicability to the police's "[commonly-]sought security camera footage," in *Carpenter*:

> [P]olice frequently contact multiple third parties with surveillance capabilities to piece together an individual's movements," and that under "the third-party doctrine . . . a defendant would ordinarily have no standing to preclude a third party from releasing" footage by which an "individual's location [is] captured on a third party's private security camera, or even network of cameras.[333]

However, the judges were concerned about "a database containing continuous video footage of every home in a neighborhood" as stifling innovation.[334] The judges warned of the potential chilling effect of self-censorship if law enforcement could install and use pole cameras without a warrant.[335]

Chief Judge Barron and Judges Thompson and Kayatta concluded that the warrantless search violated Moore-Bush's Fourth Amendment rights, but that the Government had reasonably relied on *Bucci* as binding appellate precedent and thus the motion to suppress should ultimately be denied.[336] Further, the judges indicated that the First Circuit would be mistaken if they weighed *Tuggle* over the Circuit's experience with similar issues for matters of constitutional interpretation.[337] However, by deeming the Government's warrantless, prolonged use of a pole camera aimed at a person's home a search, Chief Judge Barron and Judges Thompson and Kayatta ostensibly proscribed law enforcement from utilizing similar investigation methods without securing a search warrant.

2. Not a Search: Installing New Hardware on an Old Framework

Judges Lynch, Howard, and Gelpí sought to preserve the existing methodology decided a decade prior with "indistinguishable facts" in *Bucci*.[338] The judges applied the *Carpenter* factors to the tried-and-true two-prong privacy test and reached conclusions directly contrary to the remaining en banc panel.[339]

As a preliminary matter, Judges Lynch, Howard, and Gelpí concluded that *Carpenter*'s reference to "security cameras" meant that *Carpenter* did not

---

332. *Id.* at 352.

333. *Id.* at 352 n.27 (alterations in original) (quoting Brief for Nat'l Dist. Att'ys Ass'n as Amici Curiae Supporting Respondent at 26 & n.17, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16-402)).

334. *Id.* at 340.

335. *Id.*

336. *See id.* at 359 (holding that the government conducted a "search" through eight months of continuous footage from a fixed digital camera but relied in good faith on *Bucci*, so the exclusionary rule did not apply).

337. *See id.* at 358.

338. Under the doctrine of stare decisis, a court should not overrule its earlier decisions, absent urgent reasons and a clear manifestation of error, to promote predictability and reliance. Ramos v. Louisiana, 140 S. Ct. 1390, 1403, 1414 (2020); *Moore-Bush*, 36 F.4th at 372.

339. *See Moore-Bush*, 36 F.4th at 372.

overrule *Bucci* because the judges reasoned that "[p]ole cameras are plainly a conventional surveillance tool."[340] To demonstrate law enforcement's routine use of pole cameras and warn of the implications of endangering "other technologies extant prior to *Carpenter*," the judges cited appellate, district, and state court decisions.[341] However, the judges need not be so alarmist because Chief Judge Barron and Judges Thompson and Kayatta couched the reasonableness of Moore's expectation of privacy in her home and its curtilage.[342]

Next, the judges concluded that the CSLI in *Carpenter* was sufficiently distinct from the information gleaned from the pole camera.[343] The judges reasoned that people carry phones everywhere and their connection to the cell sites is automatic.[344] On the other hand, the judges determined that people "can take measures . . . to avoid being seen by neighbors or by passersby."[345] However, people can choose not to carry their phones to visit a place if they wish to avoid detection, but the same cannot be said if pole cameras are present, especially when aimed at their homes.[346] The judges drew the distinction that people are actively aware of their public speech and conduct when they step outside, but people may not know that their location is being shared by their cell phone service.[347]

Within *Katz*'s subjective inquiry, the judges concluded that Moore-Bush did not manifest a subjective expectation of privacy in the curtilage of her home, nor can police be expected to know Moore-Bush's privacy expectation without a showing.[348] In response to the different standards for urban–rural, wealthy–poor, and other differences that may impact a person's ability to shield

340. *Id.* at 363.

341. Since *Carpenter* was decided shortly before *Moore-Bush*, the cited pole-camera cases were primarily pre-2018. *Id.* at 364 n.36.

342. *See supra* notes 313–321 and accompanying text.

343. *Moore-Bush*, 36 F.4th at 366.

344. *Id.*

345. *Id.*

346. Individuals have rights to move and, to some extent, remain anonymous in those movements absent a subpoena, search warrant, or their exceptions. *See Carpenter*, 138 S. Ct. at 2217; United States v. Jones, 565 U.S. 400, 407–08 (2012) (preventing the government from trespassing to warrantlessly track a person's location throughout a city under common law trespass); Saenz v. Roe, 526 U.S. 489, 500–02 (1999) (identifying the components for a person's right to travel); United States v. Karo, 468 U.S. 705, 716 (1984) (prohibiting the government from using an electronic beeper—without a warrant—to know whether someone is home). *But cf.* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 342 (upholding an author's decision to remain anonymous).

347. *See Moore-Bush*, 36 F.4th at 366; Stuart A. Thompson & Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. TIMES (Dec. 19, 2019), https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html (discussing the prevalence of location tracking by private companies). Even major cell phone manufacturers warn their customers of potential privacy leaks through their devices. *See About Privacy and Location Services in iOS, iPadOS*, APPLE, https://support.apple.com/en-us/HT203033 (last visited Feb. 1, 2022) (explaining how Apple iPhone device users can control their information sharing); *Manage Your Location History*, GOOGLE, https://support.google.com/accounts/answer/3118687?hl=en (last visited Dec. 16, 2022) (explaining how Google Android device users can control their shared location information).

348. *Moore-Bush*, 36 F.4th at 367, 369.

themselves from the public view, the judges aptly point to *Katz*'s bright-line rule.[349]

Next, Judges Lynch, Howard, and Gelpí concluded that Moore-Bush's expectation of the privacy of her location, activities, and associations is not reasonable.[350] Since the judges did not find *Carpenter* to be controlling, they did not apply the three factors that the other half of the en banc panel weighed.[351]

First, the judges concluded that the information was not deeply revealing because it exposed no more than a nosy neighbor could find and copiously recall or record, especially where no fence or other structure would block their view of the front of the property.[352]

Second, the information lacked depth because the federal agents only monitored "one location," which was limited to the front (the "curtilage") of the defendant's home.[353] The information from the pole camera lacked breadth because the judges found no facts or authority to suggest that "people spend even close to the majority of their time in the curtilage of their home," so, beyond the whole of Moore-Bush's physical movements, the video only captured a sliver of her life.[354] Likewise, the information was not comprehensive because the camera was "limited to what can be viewed from the lens in its fixed position" where even a "'casual observer who is merely passing by' would have a more complete view of the entirety of the home's curtilage."[355]

Third, in addition to Moore-Bush's lack of effort to obscure the view from the public street, the judges commented that "the camera's view was sometimes obscured by foliage . . . and did not include the front door."[356] Thus, the defendant could have evaded the Government's pole camera and by extension their acquisition of information. The collection was also not automatic because the judges said "[e]ight months of pole camera surveillance cannot be generated with the push of a button and implied that this surveillance method is more costly and difficult to produce than CSLI.[357]

Having concluded that Moore-Bush failed both prongs of the reasonable expectation of privacy test, Judges Lynch, Howard, and Gelpí warned that the other concurrence runs the risk of failing to investigateand deter illegal drug and firearm transactions.[358] In particular, the judges stress the difficulty that the First

349. *Id.* at 367 (citing Katz v. United States, 389 U.S. 347, 351 (1967)) ("[T]here is no expectation of privacy in what is knowingly exposed to the public view.").

350. *Id.*

351. *See id.* at 363, 365–67.

352. *Id.* at 368.

353. *Id.*

354. *Id.* at 370 (citing United States v. Tuggle, 4 F.4th 505, 524 (7th Cir. 2021)).

355. *Id.* at 371 (Lynch, Howard & Gelpí, JJ., concurring) (quoting *id.* at 336 (Barron, C.J., Thompson & Kayatta, JJ., concurring)).

356. *Id.*

357. *See id.* at 366. *But see id.* at 372 (discussing how millions of people have equipped doorbell cameras, such as a basic model from Amazon's Ring that costs approximately fifty-two dollars).

358. *Id.* at 371.

Circuit has faced in "investigating drug conspiracies," such as identifying the conspirators, accomplices, victims, and bystanders.[359] Ignoring other investigatory tools such as those identified in Part I or their modern equivalent, Judges Lynch, Howard, and Gelpí wield stare decisis to shift Fourth Amendment rights for law enforcement despite *Carpenter*'s multi-tooled applicability.

III. CONCEPTUALIZING CAMERA SURVEILLANCE BEYOND A QUICK FIX

Since "no single rubric definitively resolves which expectations of privacy are entitled to protection," I apply both the modern trespass standard and the privacy standard to the STP's provisions for live monitoring and historical footage.[360]

A. TRESPASS STANDARD APPLIED

As the progression from *Boyd* to *Jones* shows, the scope of search is centered around privacy, albeit framed under common law trespass.[361] Although Justice Thomas would prefer to do away with *Katz* entirely, both Justice Thomas and Gorsuch's dissents in *Carpenter* invited criminal defendants to invoke their property interest.[362]

Here, the insurmountable roadblock is that the private cameras are not placed by the Government.[363] Unlike the federal agents in *Smith*, who asked the telephone companies to install the pen register, the SFPD generally does not request cameras to be installed for particular vantage points.[364] San Francisco's residents and business owners have a vested interest in optimal placement, whether their goal is to deter crime or aid in identifying criminal suspects.[365] Further, the blanket of cameras over the city may compensate for the poor view of any one camera, so the SFPD can readily bulk request the data from multiple cameras from each neighborhood coalition.[366]

Moreover, the private cameras are typically placed inside the home or affixed to the outside of the private structure. Seventy-one percent of surveyed private camera owners direct their cameras to monitor the front of their houses, which may include the front porch, driveway, or community street.[367] Thirty-

359. *See id.*

360. *See* Carpenter v. United States, 138 S. Ct. 2206, 2213–14 (2018).

361. Kerr, *supra* note 45, at 1061.

362. *See Carpenter*, 138 S. Ct. at 2236, 2264–67; Kerr, *supra* note 45, at 1049 n.9.

363. *See* Non-City STP, *supra* note 15, at 2; Bowles, *supra* note 2; Union Sq. BID, *supra* note 214, at 8–9.

364. *See* Bowles, *supra* note 2 (The San Francisco executive grants the homeowners and business owners latitude to place the security cameras where they see fit). *But see* Smith v. Maryland, 442 U.S. 735, 737 (1979) (The police requested a telephone company to install a pen register at its central office to record numbers dialed at the petitioner's home).

365. *See* Bowles, *supra* note 2.

366. *See* Union Sq. BID, *supra* note 214, at 8–9.

367. Taylor Sansano, *Home Security System Beliefs and Practices Survey 2022*, U.S. NEWS & WORLD REP. (Dec. 6, 2022, 9:00 AM), https://www.usnews.com/360-reviews/services/home-security-survey.

two percent of those surveyed use their cameras to monitor what is happening in their neighborhoods.[368]

The STP permits officers to collect videos, images, date and time, and geolocation data, or collectively, surveillance camera footage. The footage may be considered an "effect[]" that was defined as personal property other than land and buildings when the Fourth Amendment was adopted.[369] To demonstrate a property interest in the effects, one would need to prove that the collected information is more than merely personal but has commercial value.[370] For example, a celebrity may establish that an unsavory video of criminal behavior depicting themselves or a doppelgänger caused endorsement brands to drop their sponsorship; the video's commercial value may be equal to any payment by the celebrity spent for removal. In this scenario, the focus is largely on historical footage because there is no protected property interest in reputation.[371]

As for live monitoring, the issue is moot because the STP grants broad authorization to live monitor, including during exigent circumstances, significant events with a public safety concern, and investigations relating to active misdemeanor and felony violations.[372] Additionally, with "credible information of criminal activity," any high-ranked police officer can request live monitoring to investigate "specific criminal activity."[373] The cameras may be activated for a crime as minor as obstructing a sidewalk twice within twenty-four hours.[374] Under the mosaic theory, where the sum is more than its parts, the collective justifications for requested videos may amount to a trespass on effects, but only if those requests are repeatedly directed at a particular person or group of people that would rise to the level of intimidation or harassment.[375] Many individuals may not be able to suppress evidence because each video request by police may be directed at a different crime and coincidentally capture the alleged crime. Alternatively, law enforcement may file multiple requests for footage because the tendency of camera owners to send low quality of footage from adjacent cameras and a desire to efficiently develop the case.

On the other hand, the police have repeatedly proven their need to resort to live monitoring as a deterrence against crimes in progress, especially violent

368. *Id.*

369. *See* U.S. CONST. amend. IV; Maureen E. Brady, *The Lost "Effects" of the Fourth Amendment: Giving Personal Property Due Protection*, 125 YALE L.J. 946, 985 (2016) (defining "effects" according to late-eighteen century dictionaries).

370. *See* Sorrell v. IMS Health Inc., 564 U.S. 552, 579 (2011).

371. *See* Siegert v. Gilley, 500 U.S. 226, 233 (1991); Paul v. Davis, 424 U.S. 693, 701 (1976).

372. Non-City STP, *supra*, note 15 at 2.

373. *Id.*

374. S.F., CAL., POLICE CODE § 23 (2022) ("public nuisances"); Police Presentation, July 11, 2022, *supra* note 6, at 4 (The cameras may be used for "active misdemeanor and felony violations.").

375. *See, e.g.*, People v. Hollman, 590 N.E.2d 204, 209 (N.Y. 1992) (holding that police officers, in the law enforcement capacity, have broad authority to approach individuals and ask questions if they do so without intimidation or harassment).

crime.[376] More robust studies need to be conducted on the incidents of crime before and after surveillance cameras are installed to draw any conclusions.[377]

Due to the wide variety of scenarios that the police may claim to justify live monitoring and active investigations without public safety risks, the property-based test is largely inapplicable.[378] Moreover, the private cameras are placed on private property, and do not intrude upon constitutionally protected areas. This Note next turns to the privacy-based test.

B. PRIVACY STANDARD APPLIED

The flexibility of *Katz*'s two-prong privacy test has allowed the Supreme Court to develop information security for technologies from electronic beepers to thermal imaging.[379] A person traditionally did not have standing for public surveillance until *Carpenter*'s reference to the mosaic theory.[380] Previously foreclosed by the third-party and public observation doctrines, *Knotts* and *Carpenter* provide a path for recovery.[381] In *Knotts*, the Court warned of a "dragnet" as mass surveillance loomed over the public, but it was equally concerned about the prolonged surveillance of a single individual.[382] The mosaic theory emphasizes not only the human monitors scanning each live feed, but the "twenty-four hour surveillance of *any* citizen."[383] Therefore, even in the public sphere, a person may be able to suppress evidence provided they can establish a search under *Katz*'s two-prong test and meet the *Carpenter* factors.[384] The spotlight must be on the information sought, not the number of people surveilled or the duration that any individual is surveilled.

The district court's findings in *Tuggle* suggests that the plainly visible footage from San Francisco's PTZ cameras would fall outside the Fourth

376. *See supra* notes 2, 5–8 and accompanying text.

377. *See* JENNIFER KING, DEIRDRE MULLIGAN, STEVE RAPHAEL, TRAVIS RICHARDSON, JASJEET SEKHON, CTR. INFO. TECH. RSCH. INTEREST SOCIETY, U.C. BERKELEY, PRELIMINARY FINDINGS OF THE STATISTICAL EVALUATION OF THE CRIME-DETERRENT EFFECTS OF THE SAN FRANCISCO CRIME CAMERA PROGRAM 13–14 (2008) (describing an empirical study of nineteen camera sites in San Francisco between 2005 and 2008 that found no statistically significant change in property crime committed 100 feet more from a surveillance camera nor any change in violent crime within 500 feet from a camera.), *reprinted at* Nicole A. Ozer, ACLU NORCAL, *ACLU Issues New Video Surveillance Report* (Aug. 20, 2007), https://www.aclunc.org/blog/aclu-issues-new-video-surveillance-report [https://www.aclunc.org/sites/default/files/asset_upload_file796_7024.pdf].

378. Non-City STP, *supra* note 15, at 2.

379. *See* United States v. Karo, 468 U.S. 705, 716–17 (1984); Kyllo v. United States, 533 U.S. 27, 31–33 (2001); United States v. Miller, 425 U.S. 435, 442 (1976); Smith v. Maryland, 442 U.S. 735, 739–40 (1979); Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); Ferguson, *supra* note 49, at 604–05.

380. United States v. Moore-Bush, 36 F.4th 320, 340, 352 n.27 (1st Cir. 2022); *id.* at 352 n.27 (alterations in original) (quoting Brief for Nat'l Dist. Att'ys Ass'n as Amici Curiae Supporting Respondent at 26 & n.17, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16-402)).

381. *See Carpenter*, 138 S. Ct. at 2236, 2264–67; United States v. Knotts, 460 U.S. 276, 281, 283–84 (1983).

382. *See Knotts*, 460 U.S. at 281, 283–84; United States v. Maynard, 615 F.3d 544, 561–65 (D.C. Cir. 2010); United States v. Jones, 565 U.S. 400, 408–09 (2012); Renée McDonald Hutchins, *Tied Up in* Knotts*? GPS Technology and the Fourth Amendment*, 55 UCLA L. REV. 409, 446 (2007).

383. *See Knotts*, 460 U.S. at 281, 283–84; *Maynard*, 615 F.3d at 558.

384. Non-City STP, *supra* note 15 at 2.

Amendment. However, this view distorts the advances in software-based video analytics for real-time monitoring and historical videos that are inextricably intertwined with the device: human action recognition; anomaly detection; contextual understanding; emotion recognition; wide area surveillance; video search and summarization; and changing camera technologies such as depth sensors.[385] Absent signs, passing individuals may not be aware of these software-based technologies.

Video analytics may automatically alert the viewer if a person suddenly starts or stops running (as if they were running away from a crime scene), but it can also alert for more innocent behaviors like hand waving or reaching into a pocket.[386] The systems are also capable of automatically flagging user-defined anomalies, like crowd formation.[387]

More sophisticated systems, such as New York's Domain Awareness System, can tag articles of clothing with descriptors, such as "Suit_blue" for search queries, or estimate age for threat analysis during exigent circumstances.[388] Beyond facial recognition, video analytics can detect emotion from body posture.[389] In the gray area between a casual glance and peering into the intimate window of a person's life, wide-area surveillance can predict the likely movement patterns of groups of people.[390] For stored video data, the software can generate summary text that describes sequences of objects within the footage.[391] Beyond machine learning, the software can automatically manipulate PTZ cameras to track and focus on suspicious persons as they move within the camera's field of view like many smart cameras designed for pets or porches. [392]

The district court's determination that the Government did not pry into Tuggle's life for eighteen months may mean PTZ and other mechanical or digital enhancements are constitutional because the enhancements are conventional surveillance techniques used by law enforcement or, at least, their natural extensions. What is most troubling is that San Francisco's police officers may use any of these capabilities without violating the STP.[393]

In *United States v. Moore-Bush*, the First Circuit largely avoided addressing the broader category of surveillance cameras and its more complicated features.[394] Instead, both concurrences narrowly tailored the issue

385. JAY STANLEY, ACLU, THE DAWN OF ROBOT SURVEILLANCE: AI, VIDEO ANALYTICS, AND PRIVACY 12–34 (2019), https://www.aclu.org/sites/default/files/field_document/061819-robot_surveillance.pdf.

386. *Id.* at 12–14.

387. *Id.* at 16.

388. *Id.* at 18.

389. *Id.* at 24.

390. *See Carpenter*, 138 S. Ct. at 2217; STANLEY, *supra* note 385, at 27.

391. STANLEY, *supra* note 385, at 27.

392. *Id.* at 31.

393. *See* Non-City STP, *supra* note 15, at 2 (prohibiting "biometric or facial recognition technology" but not body posture, clothing, or assembly).

394. United States v. Moore-Bush, 36 F.4th 320, 361 (1st Cir. 2022) (en banc) (per curiam).

to the video recordings captured by the PTZ cameras used in the pole camera system by the federal agents.[395] The "search" group, comprised of Chief Judge Barron and Judges Thompson and Kayatta, and the "not-a-search" group, comprised of Judges Lynch, Howard, and Gelpí, had differing approaches.[396] Like the appellate court in *Tuggle*, the latter group determined that *Carpenter* was an exception to the third-party doctrine (for CSLI) rather than the rule to the reasonable expectation of privacy test.[397] The not-a-search group pointed to *Bucci* as speaking directly to the warrantless use of pole cameras, so their reliance on stare decisis is less useful in determining the appropriate measure for other jurisdictions that consider the issue as a matter of first impression.[398]

On the other side, the search group applied the mosaic theory to each prong of the subjective-objective test.[399] For the subjective prong, Chief Judge Barron and Judges Thompson and Kayatta loosely applied the mosaic theory to reach as far back as Moore-Bush's purported mindset when she decided where to live.[400] The underlying implication is that one has a greater expectation of privacy if they choose to live in a single-family, detached house as opposed to an apartment. The judges interpreted the first step of *Katz* as a low bar for the individual, provided that they do explicitly deny their right to privacy from governmental intrusion.[401]

For the second step of *Katz*, the judges concluded that Chief Justice Roberts, writing for the majority, defined the factors of reasonableness for Fourth Amendment issues as "deeply revealing," "depth, breadth, and comprehensive reach," and "inescapable and automatic."[402] Further, Chief Justice Roberts's reference to "familial, political, professional, religious, and sexual associations" in Justice Sotomayor's concurrence indicated the starting examples that rationalize the mosaic theory's new subtest.[403]

However, the search group's most compelling argument for the mosaic theory was that it could be grounded in property-based principles as alluded to by Justices Thomas and Gorsuch's dissents.[404] By emphasizing the importance of the sanctity of the home, Chief Judge Barron and Judges Thompson and Kayatta returned to the earliest interpretations of the home as "first among equals."[405]

395. *Id.*
396. *Id.*
397. *Id.* at 361.
398. *Id.*
399. *Id.* at 321.
400. *Id.* at 329.
401. *See id.* at 326 (affirming the district court's finding that the choice of residence demonstrated the defendant's subjective expectation of privacy).
402. *Id.* at 342–43.
403. *Carpenter*, 138 S. Ct. at 2217 (citing Sotomayor, J. at 2494–95).
404. *Id.* at 2241.
405. *See* Florida v. Jardines, 569 U.S. 1, 6 (2013).

To create a bright line rule that people have a reasonable expectation of privacy from cameras pointed at homes fails to acknowledge the degrees of privacy that one can reasonably expect in a single-family house, apartment, and mixed-use building.[406] San Francisco has the tenth-largest share of rental communities that include residential, office, and retail space built between 2012 and 2021 in the United States.[407] This corollary issue deserves its own analysis of the boundaries that mark the degrees of privacy in the curtilage of shared residential and business units.[408] After all, if one cannot expect privacy where one resides, where can they can expect it?

Generally, the STP authorizes use for temporary live monitoring and historical video footage.[409] The latter use grants law enforcement the authority to request records from private parties to gather evidence for a specific criminal investigation or police misconduct allegations.[410] As briefly discussed in Part III.A, since live monitoring is typically justified by exigent circumstances, I provide three recommendations for modification of the STP regarding the historical videos of the private cameras.

C. RECTIFYING THE ORDINANCE'S PRIVACY OXYMORONS FOR THE MODERN ERA

The mosaic theory's opponents argue that the theory's collective approach would be more difficult to administer than the conventional sequential approach provided by *Katz*, requires too many assumptions about the future of advanced technology in investigations, and possibly interferes with statutory privacy law.[411] Others argue that the mosaic theory is already inherent within the

406. *See* Georgia v. Randolph, 547 U.S. 103, 115 (2006); Lisa Lucile Owens, *Concentrated Surveillance Without Constitutional Privacy: Law, Inequality, and Public Housing*, 34 STAN L. & POL'Y REV 131, 139–43 (2023) (discussing the tradeoff between public safety and privacy for surveillance cameras at and near public housing in New York City, which typically impacts low-income neighborhoods); Noah Arroyo, *These Downtown S.F. Office Buildings Could Yield Thousands of Housing Units*, S.F. CHRON., https://www.sfchronicle.com/sf/article/office-conversion-housing-17769370.php (Feb. 25, 2023, 10:50 AM) (discussing how metropolitan areas are converting commercial office space to housing).

407. Andrea Neculae, *Live-Work-Play Apartments Quadrupled in 10 Years, Blending Lifestyle & Workstyle in a Post-Pandemic World*, RENTCAFE (June 14, 2022), https://www.rentcafe.com/blog/rental-market/market-snapshots/live-work-play-developments.

408. *See, e.g.*, United States v. Hopkins, 824 F.3d 726, 732 (8th Cir. 2016) (walkway outside front door of townhouse); United States v. Burston, 806 F.3d 1123, 1127 (8th Cir. 2015) (area outside apartment window, which was six feet from the walkway leading to apartment in multi-unit building); People v. Burns, 50 N.E.3d 610, 622 (Ill. 2016) (locked apartment hallway). *Cf.* State v. Kono, 152 A.3d 1, 16 (Conn. 2016) (condominiums). *But see* United States v. Jackson, 728 F.3d 367, 373–74 (4th Cir. 2013) (grass, where trashcan was located, between patio and the sidewalk in multi-building apartment complex's courtyard); United States v. Trice, 966 F.3d 506, 515 (6th Cir. 2020) (apartment hallway, where exterior door was sometimes ajar, was used by tenants as a passageway to the basement laundry unit); United States v. Sweeney, 821 F.3d 893, 901 (7th Cir. 2016) (shared basement crawlspace containing laundry machines in apartment); State v. Edstrom, 916 N.W.2d 512, 518–19 (Minn. 2018) (apartment hallway and search reasonable under state constitution).

409. Non-City STP, *supra* note 15, at 2.

410. *Id.*

411. *See* Kerr, *supra* note 38, at 346–52.

reasonable expectation of privacy test or that it runs counter to the public observation and third-party doctrines.[412]

Through its majority, concurrences, and dissents, the Supreme Court has set the groundwork to restore Fourth Amendment equilibrium between the Government's interest in criminal investigations (and deterrence) and a person's privacy rights in the digital age. Chief Judge Barron and Judges Thompson and Kayatta of the First Circuit have provided the first iteration of how the *Carpenter* factors may be integrated into the *Katz*'s two-prong test. Thus, Fourth Amendment issues regarding the definition of a "search" and what is "unreasonable" need not be based on faint-hearted originalism, but rooted in the practical impact of the use of technologies for surveillance by and for the individual and the collective.

1. Notice: Privacy in Public

The prolonged, continuous nature of cameras that are pointed at homes make the videos deeply revealing. The San Francisco ordinance should be modified to safeguard an individual's reasonable expectation of privacy by adding a notice requirement with camera stickers or adjacent signs. Posting notices limits an individual's expectation of privacy, but the stickers and adjacent signs afford an individual the opportunity to decide how they may conduct themselves in recorded public spaces. Further, the presence of visible security signs and cameras are effective burglary deterrents because over 40 percent and 60 percent of incarcerated offenders, respectively, consider these security measures for the suitability of a target home or business.[413]

For street-facing cameras that incidentally capture the inside of another's home, mandatory stickers and signage inform strangers to the innocuous behavior, such that residents can draw their blinds in densely populated metropolitan areas or plant privacy hedges in suburban or rural areas. For passing visitors, the signage allows individuals to plan subsequent routes around the recorded area or avoid the area entirely. Whether an individual is planning criminal activity, the desire to remain "off-the-grid" may not be outlandish as police agencies have unprecedented access to video surveillance systems, such as Amazon's Ring, by voluntary transmittals or search warrants.[414] Despite

412. 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, 398–411 (2013).

413. Neighborhood Watch and beware-of-dog signs were only considered by burglars less than twenty-five percent of the time, but the presence of people inside a home or business ultimately deterred about sixty percent of offenders. JOSEPH B. KUHNS, KRISTIE R. BLEVINS & SEUNGMUG "ZECH" LEE, UNDERSTANDING DECISIONS TO BURGLARIZE FROM THE OFFENDER'S PERSPECTIVE 31–32, 41 (Univ. N.C. at Charlotte Dep't Crim. Just. & Criminology, Alex Sawyers & Brittany Miller eds., 2012) (discussing how most offenders considered several factors whether the burglary was planned and evaluating their effectiveness).

414. *Compare* BARRY FRIEDMAN, FARHANG HEYDARI, MAX ISAACS & JULIAN CLARK, RING NEIGHBORS & NEIGHBORS PUBLIC SAFETY SERVICE: A CIVIL RIGHTS & CIVIL LIBERTIES AUDIT 21 (N.Y.U. Policing Project ed., 2021) (acknowledging "the nearly 2,000 policing agencies" that downloaded videos from Ring systems, but

Ring's third-party audit, the ready access to continuously recording devices, especially those that can use artificial intelligence to play back video segments, enable police to track a person's whereabouts.[415] Multiple five-second recordings of a neighbor's car driving by a Ring doorbell camera in a two-hour span provided sufficient "suspicious activity" for an Ohio court to issue a warrant for footage from the owner's twenty cameras.[416]

Certain paths may be unavoidable, especially for individuals with only one practical path of egress to their home. With mandatory notice of recording, the reasonable expectation of privacy still operates on a sliding scale, but it is defined by whether they are neighborhood residents or passing strangers. This preliminary step mitigates residential-type issues pertaining to the reasonable expectation of privacy leveling as discussed in Part III.B and III.C. Instead, the step breathes new life into *Katz*'s subjective prong by weighing whether the defendant manifested their subjective expectation of privacy by their conduct and proximity to their home. For example, an individual would not manifest their expectation of privacy when playing basketball in the street of their cul-de-sac. Additionally, an individual driving one block away toward their home may satisfy the subjective prong in the sense that many individuals would prefer not to be followed to the final block of their typical route home.[417] Conversely, this subjective expectation of privacy may be lessened if multiple routes to one's home are available.

For private surveillance cameras, the mandatory camera stickers and adjacent signs reduces the guesswork of the subjective prong to their conduct as it relates to their location or *intended* destination. Yet, the combination of private cameras aimed at homes and the "always on" nature of the cameras bought by the cryptocurrency mogul chip away at what may be reasonable depending on

---

failing to disclose how many videos members of the public voluntarily shared videos with police), *with* CONSUMER REPORTS, JANUARY 2021 RESULTS—CREDIT REPORTS ERRORS, VIDEO DOORBELLS, AND PRODUCT SAFETY RECALL ITEMS 6 (CR Surv. Rsch. Dep't. ed., 2021) (noting that 10% of doorbell camera owners shared footage with law enforcement, 12% of respondents did not despite "hav[ing] reason to consider doing so," and 79% of respondents not having a reason to do so).

415. *See, e.g.*, *Event and 24/7 Video History*, GOOGLE NEST, https://support.google.com/googlenest/answer/9681538/#3-hour-ebr (last visited May 26, 2023) (discussing notification and review features when "sound and video events," such as humans, animals, and cars, are detected); *Ring Protect*, RING, https://ring.com/protect-plans (last visited May 26, 2023) (discussing similar notification and review features with customization options).

416. *See* Alfred Ng, *The Privacy Loophole in Your Doorbell*, POLITICO (Mar. 7, 2023, 4:30 AM), https://www.politico.com/news/2023/03/07/privacy-loophole-ring-doorbell-00084979.

417. Sam Sabin, *People Uncomfortable With Government Tracking, but Less So if It's to Fight Virus*, MORNING CONSULT PRO (Mar. 23, 2020, 4:48 PM), https://pro.morningconsult.com/articles/coronavirus-location-data-tracking (finding that 25% of U.S. adults were comfortable with the government using location data to generally track them as compared to 67% that were uncomfortable). *But see* Andrew Laningham, *Are Location Sharing Features More Than a Convenient Tool?*, HARRIS POLL (Aug. 22, 2022), https://theharrispoll.com/briefs/location-sharing-features/ (finding that 79% of U.S. adults report that they have location sharing features activated on their phones and other devices some time as compared to 16% that always having location features turned on).

the duration of access to live surveillance (for the purpose of spying on neighbors or passing visitors) or historical records.[418]

2. Brief Descriptive Justification: Closed Captions Absent Audio

The ordinance creates a mass surveillance network due to its depth, breadth, and comprehensive reach to all residents and visitors. Currently, live monitoring is permitted during exigent circumstances, public safety concerns such as crowd sizes, and investigations with the approval of high-ranked police officer whereas historical footage is limited to investigations (without authorization) of criminal matters and police misconduct. [419] *Katz*'s objective prong guides the analysis by requiring police officers to provide notice and obtain authorization from stakeholders. The oversight by a civilian and an additional police officer helps mitigate against the risk of a dragnet, especially given the multitude of ways that law enforcement can access data.[420]

First, the STP should be modified to require police officers to provide camera owner with a brief, written description with each video request. The description should be grounded by a "reasonable, articulable suspicion that criminal activity is afoot."[421] The *Terry* standard is less demanding than probable cause and "requires a showing considerably less than preponderance of the evidence."[422] Rather, it reinforces the rights of private camera owners to terminate their existing agreement with the SFPD if the owners suspect the Department is disproportionately targeting marginalized communities and curtailing First Amendment rights.[423] Further, officers would be discouraged from submitting repeated requests for access to live-monitoring or bulk requests for historical footage. On the contrary, officers are incentivized to provide more detail to private camera owners because the owners may more efficiently sort through minutes or hours of footage by software to locate pertinent clips.[424] For example, "an individual suspected of a hit-and-run was driving a white pickup truck" on a certain date may allow a private camera owner to filter notifications of all vehicles passing before their doorbell camera as opposed to the back-and-forth requests for the particular event. Thus, the proposed notice requirement fosters community engagement.

Second, the STP should require authorization by a high-ranked officer for *all* live-monitoring. Since officers would be required to provide notice to the

418. *See* Bowles, *supra* note 2.

419. Non-City STP, *supra* note 15, at 2.

420. *See* Johana Bhuiyan, *How can US Law Enforcement Agencies Access Your Data? Let's Count the Ways*, GUARDIAN (Apr. 4, 2022, 10:05 AM EST), https://www.theguardian.com/technology/2022/apr/04/us-law-enforcement-agencies-access-your-data-apple-meta (discussing the whack-a-mole approach to protecting one's data from technology companies and the government); *see also supra* note 347 and accompanying text.

421. *See* Illinois v. Wardlow, 528 U.S. 119, 123 (2000) (citing Terry v. Ohio, 392 U.S. 1, 30 (1968)).

422. *Id.*

423. *See supra* notes 8–11 and accompanying text.

424. *See supra* text accompanying note 223; *see also supra* note 414.

private camera owners for each request, police may submit a duplicate with a case identification number to provide more context on the investigation using internal police systems. Therefore, implementing the *Terry* standard would not substantially hamper the investigation or other officer duties. Further, duplicating the notice to the private camera owner increases transparency.

Despite the reliance on *Katz*, the recommendations are inextricably tied to duration. Thus, the recommendations cannot be adopted independently.

3. Duration Limitations: The "Neverending" Feed

The wide degree of latitude with which law enforcement may access cameras to monitor in real-time, the duration of each granted access, and the recording capabilities of many cameras make police's collection of information inescapable and automatic. Like the cellular retention policies of CLSI in *Carpenter*, the STP prevents the wholesale download of personally identifiable information and limits potentially relevant data to "two years from the last date of entry" unless the investigation is ongoing or maintenance is otherwise required by the law.[425] Further, SFPD is prohibited from "recording or duplicating the live monitoring feed using any electronic device."[426] Thus, any receipt—live or historical—may be evidence that they did not already possess. Unlike the three-camera surveillance system in *Moore-Bush*, the network of over 1,000 cameras, each with a set of features that may extend beyond pan, tilt, and zoom and sometimes redundant for a particular directed area, paints a detailed, encyclopedic, and effortlessly compiled picture of any individual's movements across San Francisco.[427] The monitoring of George Floyd protestors proved as much.[428] However, modern configurations of conventional surveillance technologies are not immune to the subpoena and search warrant requirement.[429]

Unlike a mere three-camera pole camera system directed at one area for one individual in *Moore-Bush*, specific cameras can be "activated" by accessing real-time feeds or historical data along a certain path. For example, if law enforcement knows that a suspect is heading South on Market Street from the Ferry Building, law enforcement can leapfrog between feeds or request data sequentially to develop a record of the suspect's location. While law enforcement's conduct would likely be justified for a bomb threat, the reasonability of the surveillance efforts is inversely correlated with the seriousness of the crime as time passes.

For real-time access, each period should be limited to twelve-hour increments with no more than two extensions for each ongoing matter. This would permit police to conduct surveillance during exigent circumstances with

425. *See supra* notes 326–328 and accompanying text.

426. Non-City STP, *supra* note 15, at 2.

427. *See supra* notes 210217 and accompanying text; *see also* Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018).

428. *See supra* note 9 and accompanying text.

429. *See* discussion *supra* Part 1.B.3.

sufficient time to obtain a subpoena or search warrant. Further, this twelve-hour span would allow police to respond to impromptu security concerns if crowds formed during protests without chilling speech.

For historical footage, each period should be limited to twenty-four hours with no more than two extensions for each ongoing matter. The STP should not be used as a means for a fishing expedition of potentially criminal activity. Rather, sustained community-oriented policing with officers on the ground increases legitimacy and the public's willingness to cooperate in investigations.[430]

Though Chief Judge Barron and Judges Thompson and Kayatta in *Moore-Bush* did not find duration dispositive, duration remains an instructive guide to defining whether a Fourth Amendment search occurred. When faced with new technologies that obtain video, audio, and other evidence to varying degrees of depth, breadth, and comprehensive reach, the duration of police conduct helps delineate reasonable expectations of privacy into subjective efforts to maintain that privacy and those that are objectively reasonable.

CONCLUSION

Although the San Francisco Surveillance Technology Policy is likely constitutionally sufficient, this Note provides the development of how it and surveillance cameras across the nation may be assessed under a new framework. This Note recommends requiring notice, justification, and strict-time limits (to real-time surveillance and historical footage) to better protect an individual's reasonable expectation of privacy. The recommendations work in tandem to balance the competing interests of the individual and the collective. Specifically, as new surveillance technologies emerge and new applications of existing devices are developed, individuals and local communities should retain control of the flow of their data to law enforcement. On the other hand, law enforcement agencies should not be curtailed to the extent that their legitimate efforts to investigate criminal activity is halted entirely. Local communities and law enforcement must work together to protect privacy and public safety alike.

430. Kyle Peyton, Michael Sierra-Arévalo & David G. Rand, *A Field Experiment on Community Policing and Police Legitimacy*, 116 PROC. NAT'L ACAD. SCI. 19894, 19897 (2019).