2022

Persistent Surveillance

Andrew Guthrie Ferguson

PERSISTENT SURVEILLANCE

Andrew Guthrie Ferguson

PERSISTENT SURVEILLANCE

*Andrew Guthrie Ferguson**

Persistent surveillance technologies grant police vast new investigative capabilities. The technologies both monitor targeted areas and generate databases of searchable information about people, places, and patterns that can be connected and accessed for criminal prosecutions.

In the face of this growing police surveillance, courts have struggled to make sense of a fragmented Fourth Amendment doctrine. The Supreme Court has offered some clues that "digital may be different" when it comes to surveillance, but lower courts have been left struggling to apply old law to new technologies. Warrantless use of persistent surveillance technologies raises hard questions about when a "search" occurs and whether the Fourth Amendment should limit overbroad police collection.

This Article attempts to solve the persistent surveillance puzzle. First, it defines persistent surveillance technologies and explains why these policing systems represent a different privacy and security threat—one constitutionally distinguishable from traditional policing tools. Second, the Article examines the legal questions courts must ask in evaluating the Fourth Amendment implications of new persistent surveillance technologies used without a warrant. This Part synthesizes lessons learned from recent Supreme Court cases on digital surveillance and offers a new framework for future analysis. Third, this Article examines the technological framing questions courts must ask in evaluating these networked systems. Revealingly, how courts choose to define the scope, scale, and capacity of the technology itself—what I call the unit of surveillance—will shape the Fourth Amendment answers.

The long-term goal of this Article is to offer a Fourth Amendment framework for all future persistent surveillance technologies. The short-term project applies these principles to two vexing persistent surveillance puzzles recently before the federal courts involving aerial surveillance planes and long-term pole cameras.

INTRODUCTION

Video-equipped spy planes that can record an entire city.[1] Digital pole cameras that never turn off.[2] A data grid that tracks and preserves location.[3] These are the new realities of digital surveillance: technologies that are massive in scope, enduring in memory, retrospective, pervasive, and persistent.[4] The nature of police surveillance has changed, and the question is whether the Fourth Amendment can catch up.[5]

---

* Professor of Law, American University Washington College of Law. Thank you to Ngozi Okidegbe, Wayne Logan, Stephen Henderson, Matthew Tokson, Barry Friedman, and Farhang Heydari for comments on earlier drafts of this Article.

1. *See* Monte Reel, *Secret Cameras Record Baltimore's Every Move from Above*, BLOOMBERG BUSINESSWEEK (Aug. 23, 2016), http://www.bloomberg.com/features/2016-baltimore-secret-surveillance.

2. Matthew Tokson, *The Next Wave of Fourth Amendment Challenges After* Carpenter, 59 WASHBURN L.J. 1, 18 (2020) (discussing pole cameras as continuous searches).

3. Note*, Geofence Warrants and the Fourth Amendment*, 134 HARV. L. REV. 2508, 2512 (2021).

4. For more background on the development of big data surveillance technologies, see ANDREW GUTHRIE FERGUSON, THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, AND THE FUTURE OF LAW ENFORCEMENT (2017) (detailing the growing of big data surveillance).

5. The Fourth Amendment provides that:

This Article addresses how courts should approach warrantless persistent surveillance.[6] Persistent surveillance raises different questions than traditional surveillance because the technologies operate at a different scale, duration, and reach than traditional investigative techniques.[7] A plane that can record an entire city is simply not the same thing as a plane that flies over a single backyard.[8] A network that captures all cell phone locations is not the same thing as a device that finds one phone's location.[9] Yet, Fourth Amendment law has not fully recognized this shift in systemic surveillance capacity, and courts have struggled to adapt old law to new technologies.[10]

This Article offers three insights into the evolving application of Fourth Amendment principles to new policing technologies. First, it defines persistent surveillance technologies and explains why these policing systems represent a different privacy and security threat—one that is constitutionally distinguishable from traditional policing tools.[11] Second, the Article examines the legal and technological questions courts must ask in evaluating the Fourth Amendment implications of new persistent surveillance technologies used without a warrant.[12] This Part synthesizes lessons learned from recent Supreme Court cases on digital surveillance and offers a new framework for future analysis. In addition, this Part examines the technological framing questions courts must ask in evaluating these networked systems.[13] How courts define the scope, scale, and capacity of the technologies—what I call the unit of surveillance—will shape the constitutional answers. Third, this Article will use two recent federal court cases as examples of how to resolve the constitutional questions of long-term persistent surveillance.[14] The first case involves the Persistent Surveillance System planes that flew over Baltimore, Maryland

---

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

U.S. CONST. amend. IV.

6. It is important to note this Article's focus on *warrantless* surveillance, as the discussion largely turns on analyzing the threshold question of whether there was a "search" for Fourth Amendment purposes.

7. *See infra* Part I (discussing why digital persistent surveillance is a different act with different harms than traditional surveillance).

8. These distinctions will be discussed in Part II.

9. *Cf.* Stephanie K. Pell & Christopher Soghoian, *A Lot More Than a Pen Register, and Less Than a Wiretap: What the StingRay Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities*, 16 YALE J.L. & TECH. 134, 144–48 (2013) (discussing the capabilities of StingRay devices to find individual phones).

10. *See infra* Part II (discussing the Supreme Court's attempts to address new surveillance technologies in the Fourth Amendment context).

11. *See infra* Part I.

12. *See infra* Part II.

13. *See infra* Part II.

14. *See infra* Part III.

recording the entire city in daily bursts.[15] The second case involves long-term digital pole cameras that can record homes for months (or years) at a time.[16]

The goal of this Article is to offer a Fourth Amendment framework for all future persistent surveillance technologies used by police without a warrant.

I. PERSISTENT SURVEILLANCE TECHNOLOGIES

"Persistent surveillance"[17] is a generic term that encompasses a basket of surveillance systems that share two commonalities. First, the technologies are broad and/or deep in scale and scope—for example monitoring a wide area (a city) and/or monitoring a narrow area (a home) for long periods of time.[18] Second, the technologies allow for continuous digital collection which, when saved, allows for retrospective searches of images, people, patterns, or events.[19]

A. Persistent Surveillance Technologies Defined

As will be discussed in this Part, persistent surveillance systems can be divided up into three subcategories: (1) technologies that involve individualized, targeted surveillance without generalized monitoring capabilities (for example, affixing a global positioning system (GPS) device[20] on a particular car for a long period of time); (2) technologies that involve generalized surveillance without individualized targeting (for example, installing GPS tracking capabilities on all cars); and (3) technologies that allow individualized targeted searches from generalized surveillance capabilities (for example, being able to search for a particular car within the saved database of GPS coordinates for all cars). Many criminal investigations and prosecutions involve questions around the first and third subcategories and each will be discussed in the next three Subparts.[21]

---

15. Leaders of a Beautiful Struggle v. Balt. Police Dep't, 2 F.4th 330, 333 (4th Cir. 2021).

16. United States v. Tuggle, 4 F.4th 505, 511 (7th Cir. 2021).

17. As Professor Margot Kaminski once elegantly explained the concept, "Persistent and targeted surveillance collapses individual moments of interaction, spread out over time and mitigated through human forgetfulness, into one long story of an individual's life." Margot E. Kaminski, *Privacy and the Right to Record*, 97 B.U. L. REV. 167, 215 (2017) (describing the recognized harm of persistent surveillance).

18. As will be discussed, this type of surveillance shares certain commonalities but does not have a fixed definition.

19. As will be discussed, the technical realities of digital persistent surveillance help define a certain type of surveillance technology that is distinguishable from other forms of traditional analog surveillance.

20. Lenese C. Herbert, *Challenging the (Un)Constitutionality of Governmental GPS Surveillance*, CRIM. JUST., Summer 2011, at 34, 35 (describing how GPS technology works); Renée McDonald Hutchins, *Tied Up in* Knotts*? GPS Technology and the Fourth Amendment*, 55 UCLA L. REV. 409, 449 (2007) (discussing the Fourth Amendment considerations).

21. As an example, the Supreme Court decided *United States v. Jones* which involved the use of a GPS device attached to the defendant's family vehicle. United States v. Jones, 565 U.S. 400, 402 (2012). Other cases involve requests (via warrant or subpoena) for OnStar GPS data. *See, e.g.*, Nathan J. Buchok, Note, *Plotting a Course for GPS Evidence*, 28 QUINNIPIAC L. REV. 1019, 1025–26 (2010) ("The OnStar system uses GPS and cellular technology to connect the vehicle to the OnStar center. At the OnStar center, advisors can use GPS technology to determine the location of the vehicle and send help if it is in an accident. . . . Law

1. Individualized Targeted Surveillance Technologies: Defined

Police have used individualized targeted surveillance technologies for decades.[22] Microphones, beepers, thermal imaging devices, and other technologies have allowed police to investigate people suspected to be involved in criminal activities.[23] This Article focuses on the subset of these technologies that allow for persistent surveillance. "Persistent" in the individualized context means monitoring that is long term, aggregating of information, and retrospective.[24] As mentioned, a good example of such a technology is GPS tracking. Police can affix a GPS tracking device on an object (or car) and monitor its movements for an extended period of time.[25] In addition, pole cameras—fixed video cameras that monitor a home for months or years—are another example of an individualized surveillance tactic that falls into the category of individualized targeted surveillance.[26]

Technology-enhanced, individualized persistent targeted surveillance creates real privacy risks.[27] Because of this fact, the Supreme Court has been receptive to legal challenges to warrantless use.[28] Some longer-term GPS tracking, all thermal imaging of a home, and electronic wiretaps require a warrant.[29] At the same time, current constitutional law allows for significant monitoring using enhanced surveillance in public places, around individual

enforcement officials can subpoena OnStar service providers to provide GPS data about a car's location much in the same way they can subpoena cellular phone service providers." (footnotes omitted)).

22. *See generally* Alvaro M. Bedoya, *The Color of Surveillance*, SLATE (Jan. 18, 2016, 5:55 AM), https://slate.com/technology/2016/01/what-the-fbis-surveillance-of-martin-luther-king-says-about-modern-spying.html; SIMONE BROWNE, DARK MATTERS: ON THE SURVEILLANCE OF BLACKNESS 12–17 (2015). Many scholars have critiqued the growing use of surveillance technologies for reifying structural inequality and carceral power. *See, e.g.*, RUHA BENJAMIN, RACE AFTER TECHNOLOGY: ABOLITIONIST TOOLS FOR THE NEW JIM CODE (2019); Vincent M. Southerland, *The Intersection of Race and Algorithmic Tools in the Criminal Legal System*, 80 MD. L. REV. 487, 498 (2021); Ngozi Okidegbe, *Discredited Data*, 107 CORNELL L. REV. (forthcoming 2022).

23. *See, e.g.*, Olmstead v. United States, 277 U.S. 438, 465–66 (1928) (wiretaps), *overruled by* Katz v. United States, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967); *Katz*, 389 U.S. at 353 (wiretaps); Smith v. Maryland, 442 U.S. 735, 744–45 (1979) (pen register); United States v. Knotts, 460 U.S. 276, 282 (1983) (electronic beeper); United States v. Karo, 468 U.S. 705, 715 (1984) (electronic beeper); Kyllo v. United States, 533 U.S. 27, 34–35 (2001) (thermal imager).

24. *See* Kaminski, *supra* note 17.

25. Herbert, *supra* note 20, at 35.

26. Ron LaPedis, *How to Use Video Surveillance Camera Systems to Monitor Crime Hot Spots*, POLICE1 (July 20, 2018), https://www.policeone.com/police-products/radios/surveillance/articles/476978006-How-to-use-video-surveillance-camera-systems-to-monitor-crime-hot-spots/.

27. Danielle Keats Citron & David Gray, *Addressing the Harm of Total Surveillance: A Reply to Professor Neil Richards*, 126 HARV. L. REV. F. 262, 265 (2013).

28. *See infra* the cases discussed in Part III.

29. *See* United States v. Jones, 565 U.S. 400, 402 (2012) (GPS); Kyllo v. United States, 533 U.S. 27, 34–35 (thermal imaging); 18 U.S.C. § 2518(4) (wiretaps).

property (outside the home), and most short-term location tracking without a warrant.[30]

Notably, for purposes of this definitional Subpart, individualized persistent targeted surveillance involves suspicion of particular people for long periods of time which may include aggregating many bits of information about particular people or locations.

2. Generalized Surveillance Technologies: Defined

Generalized surveillance technologies are expanding across American cities.[31] Networks of linked video surveillance cameras record the daily happenings in Chicago, Detroit, and New York City.[32] Audio sensors listen for gunshots in Chicago, Washington D.C., and San Diego.[33] Automated License Plate Readers (ALPR) record the location of cars in dozens of cities.[34] Cell phones, smartphone applications, and almost every smart car can be tracked by sophisticated networks of geolocation technologies.[35] Some of these systems are run by police, some by private companies, and some operate in partnership

30. Marc Jonathan Blitz, *The Fourth Amendment Future of Public Surveillance: Remote Recording and Other Searches in Public Space*, 63 AM. U. L. REV. 21, 79 (2013) (recognizing that "police surveillance in public has traditionally been entirely outside the Fourth Amendment's coverage").

31. *See* SARAH BRAYNE, PREDICT AND SURVEIL: DATA, DISCRETION, AND THE FUTURE OF POLICING 8-11, 41 (2021); JAY STANLEY, THE DAWN OF ROBOT SURVEILLANCE: AI, VIDEO ANALYTICS, AND PRIVACY 17–21 (2019), https://www.aclu.org/sites/default/files/field_document/061819-robot_surveillance.pdf. These developments have been met with resistance from community activists who have sought to defund and expose the power of new surveillance technologies. *See, e.g.*, DEFUND SURVEILLANCE, https://www.defundsurveillance.org/ (last visited Sept. 16, 2022); *Fuck the Police, Trust the People: Surveillance Bureaucracy Expands the Stalker State*, STOP LAPD SPYING COAL. (June 24, 2020), https://stoplapdspying.org/surveillance-bureaucracy-expands-the-stalker-state/.

32. *See* Timothy Williams, *Can 30,000 Cameras Help Solve Chicago's Crime Problem?*, N.Y. TIMES (May 26, 2018), https://www.nytimes.com/2018/05/26/us/chicago-police-surveillance.html; Amy Harmon, *As Cameras Track Detroit's Residents, a Debate Ensues Over Racial Bias*, N.Y. TIMES (July 8, 2019), https://www.nytimes.com/2019/07/08/us/detroit-facial-recognition-cameras.html; Alan Feuer, *Council Forces N.Y.P.D. to Disclose Use of Drones and Other Spy Tech*, N.Y. TIMES (June 18, 2020), https://www.nytimes.com/2020/06/18/nyregion/nypd-police-surveillance-technology-vote.html.

33. Todd Feathers, *More Cities Are Moving to Drop Automated Gunshot-Detection Tech*, VICE (Aug. 3, 2021, 8:00 AM), https://www.vice.com/en/article/88nekp/more-cities-are-moving-to-drop-automated-gunshot-detection-tech; *Shot Spotter Gun Shots*, OPEN DATA DC, https://opendata.dc.gov/datasets/DCGIS::shot-spotter-gun-shots/about (last visited Sept. 16, 2022). *See generally* POLICING PROJECT AT N.Y. UNIV. SCH. OF L., PRIVACY AUDIT & ASSESSMENT OF SHOTSPOTTER, INC.'S GUNSHOT DETECTION TECHNOLOGY (2019).

34. Bryce Clayton Newell, *Local Law Enforcement Jumps on the Big Data Bandwagon: Automated License Plate Recognition Systems, Information Privacy, and Access to Government Information*, 66 ME. L. REV. 397, 404–11 (2014).

35. Jennifer Valentino-DeVries et al., *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret,* N.Y. TIMES (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html; *see also* Adrienne LaFrance, *How Self-Driving Cars Will Threaten Privacy*, ATLANTIC (Mar. 21, 2016), https://www.theatlantic.com/technology/archive/2016/03/self-driving-cars-and-the-looming-privacy-apocalypse/474600/; Geoffrey A. Fowler, *What Does Your Car Know About You? We Hacked a Chevy to Find Out*, WASH. POST (Dec. 17, 2019, 7:00 AM), https://www.washingtonpost.com/technology/2019/12/17/what-does-your-car-know-about-you-we-hacked-chevy-find-out/.

together.[36] As public safety monitoring techniques, these technologies largely have avoided constitutional scrutiny because their collection happens pre-investigation and the technologies do not always result in evidence introduced in criminal cases.[37] While these technologies have (on occasion) been used in criminal prosecutions, the creation of the networks of generalized surveillance have escaped sustained legal challenge.[38] Just having the cameras running or the sensors listening or satellites mapping—alone—has not triggered sustained Fourth Amendment litigation.[39]

Generalized surveillance technologies, thus, create generalized privacy and security fears but remain difficult to litigate against without cognizable individual privacy or constitutional harms. Anyone can be tracked camera-to-camera as they walk down the streets in downtown Chicago, or tracked step-by-step by the smartphone in their pocket, but there is not a clear Fourth Amendment violation in its generalized mass surveillance state.[40] As will be discussed with the Persistent Surveillance System planes in Baltimore, the privacy harms are real, but litigating them has been difficult because of standing and other judge-made limitations arising from current Fourth Amendment doctrine.[41]

As a definitional concept, however, it is important to understand what generalized persistent surveillance technologies allow. As networks of cameras, sensors, or location data, these systems create the capacity for large scale surveillance that can be used by law enforcement to investigate individual crimes (even if many times the surveillance is just monitoring and not used for

36. Private companies like Palantir essentially manage the data systems for public police departments like the LAPD. *See* Mark Harris, *How Peter Thiel's Secretive Data Company Pushed into Policing*, WIRED (Aug. 9, 2017, 9:40 AM), https://www.wired.com/story/how-peter-thiels-secretive-data-company-pushed-into-policing; Matt Burns, *Leaked Palantir Doc Reveals Uses, Specific Functions and Key Clients*, TECHCRUNCH (Jan. 11, 2015, 6:37 PM), https://techcrunch.com/2015/01/11/leaked-palantir-doc-reveals-uses-specific-functions-and-key-clients/.

37. Elizabeth E. Joh, *The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing*, 10 HARV. L. & POL'Y REV. 15, 33, 39 (2016).

38. This does not mean these technologies have escaped criticism. Academics and activists have raised concern about the growth of surveillance technologies. *See, e.g.*, Brendan McQuade, *Police Surveillance is Criminalization and it Crushes People*, COUNTERPUNCH (Oct. 15, 2020), https://www.counterpunch.org/2020/10/15/police-surveillance-is-criminalization-and-it-crushes-people/; Shakeer Rahman & Brendan McQuade, *Police Bureaucracy and Abolition: Why Reforms Driven by Professionals Will Renew State Oppression*, COUNTERPUNCH (Sept. 17, 2020), https://www.counterpunch.org/2020/09/17/police-bureaucracy-and-abolition-why-reforms-driven-by-professionals-will-renew-state-oppression/.

39. *See generally* BARRY FRIEDMAN, UNWARRANTED: POLICING WITHOUT PERMISSION 143–84 (2017).

40. Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment*, 105 MINN. L. REV. 1105, 1128 (2021) ("Most Fourth Amendment cases arise in the criminal context through a suppression hearing, so general challenges to generalized police powers are non-justiciable due to a lack of standing.").

41. *See generally* Christopher Slobogin, *Standing and Covert Surveillance*, 42 PEPP. L. REV. 517, 530 (2015) (describing justiciability requirements for Fourth Amendment litigation).

prosecution).[42] The camera or audio sensor can be used to prosecute individuals, even if that is not the primary purpose. Such a transformation of the built architecture of surveillance into a targetable prosecution tool is the subject of the next Subpart.

3. Targetable Surveillance Technologies: Defined

Generalized surveillance capabilities can be transformed into particularized evidence because the networks of surveillance are capturing criminal activity (along with everything else). Unlike traditional, individualized surveillance, in which the police officer intentionally had to direct the camera toward the suspect's home or install the GPS device on a suspect's car, the technology already exists with persistent systems of surveillance (and is always turned on).[43] The camera has already captured the relevant footage, or the GPS coordinates have already been recorded. All police need to do is search the dataset to find the needed evidence.

Almost all generalized surveillance technologies—once digitized—can be turned into to targetable surveillance. Video networks can identify individual actors on the scene with a quick search.[44] Gunshots can be tracked to a particular corner.[45] Cell site location tracking has already played a starring role in the Supreme Court's Fourth Amendment evolution with *Carpenter v. United States*, a case in which already collected cell phone location data was used to connect Mr. Carpenter to a crime.[46] In addition, persistent surveillance planes and facial recognition from cameras offer new ways to track individuals suspected of criminal activity across camera networks.[47] In each case, the broader, continuously-recording, digital surveillance system captures the needle in the haystack along with millions of bits of hay. And because the Fourth Amendment has largely focused on collection and not use of that information,

---

42. Note, *supra* note 3.

43. As will be discussed, this "always-on" automated function is a key distinguishing factor of new persistent surveillance technologies. *See infra* Part I.C.

44. Jake Laperruque, *Preventing an Air Panopticon: A Proposal for Reasonable Legal Restrictions on Aerial Surveillance*, 51 U. RICH. L. REV. 705, 717 (2017) ("[T]he tracking technology, BriefCam, allows law enforcement to overlay hours of video and then isolate individuals based on certain factors so monitors can view all applicable targets with hours of time reduced to minutes. . . . With such technologies, police could 'reverse-engineer' location tracking, picking a route they want to monitor, then use BriefCam to immediately isolate and identify everyone who used it over the course of several hours." (footnotes omitted)).

45. Veronique Greenwood, *New Surveillance Program Listens for Gunshots, Get Police There in Minutes*, DISCOVER MAG. (May 30, 2012, 4:09 PM), https://www.discovermagazine.com/technology/new-surveillance-program-listens-for-gunshots-get-police-there-in-minutes; *see also* State v. Hill, 851 N.W.2d 670, 690–91 (Neb. 2014) (allowing ShotSpotter evidence to be introduced into trial).

46. Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018).

47. *See* Ferguson, *supra* note 40, at 1122 ("After a crime, police may wish to run a face image they possess against stored video surveillance from a network of city cameras. The same matching technology can be used to search months of stored surveillance footage, networks of video feeds, or growing image databases for images to compare with the target's face." (footnotes omitted)).

there exists an open question of whether the Constitution should apply at all to protect using such already collected personal information.[48]

The next Part looks at two specific cases where federal courts of appeal have wrestled with questions of persistent surveillance. The United States Court of Appeals for the Fourth Circuit struck down the targetable surveillance technology of Persistent Surveillance System planes in Baltimore, Maryland.[49] In contrast, the United States Court of Appeals for the Seventh Circuit allowed the individualized surveillance technique of a long-term (eighteen-month) pole camera to survive a Fourth Amendment challenge.[50]

B. Persistent Surveillance in Application

In the summer of 2021, the en banc United States Court of Appeals for the Fourth Circuit held that aerial surveillance planes flying over Baltimore and routinely recording hours of video footage (without a warrant) violated the Fourth Amendment.[51] In that same summer, the United States Court of Appeals for the Seventh Circuit held that a digital pole camera monitoring a home continually for eighteen months (without a warrant) did not violate the Fourth Amendment.[52] These two cases—fueled by new digital surveillance capabilities—raise challenging questions about how Fourth Amendment protections should evolve to meet persistent surveillance threats.

1. Warrantless Persistent Aerial Surveillance

First in 2016, and then again in 2020, the Baltimore Police Department (BPD) flew aerial surveillance planes with sophisticated cameras able to record and track any object observable in public.[53] In partnership with a private company, Persistent Surveillance Systems (PSS), initially funded by the

48. *See, e.g.*, Rebecca Lipman, *Protecting Privacy with Fourth Amendment Use Restrictions*, 25 GEO. MASON L. REV. 412, 440 (2018).

49. Leaders of a Beautiful Struggle v. Balt. Police Dep't, 2 F.4th 330, 333 (4th Cir. 2021).

50. United States v. Tuggle, 4 F.4th 505, 516 (7th Cir. 2021).

51. *Leaders of a Beautiful Struggle*, 2 F.4th at 346 ("The [Aerial Investigation Research (AIR)] program records the movements of a city. With analysis, it can reveal where individuals come and go over an extended period. Because the AIR program enables police to deduce from the whole of individuals' movements, we hold that accessing its data is a search, and its warrantless operation violates the Fourth Amendment.").

52. *Tuggle*, 4 F.4th at 511 ("In short, the government's use of a technology in public use, while occupying a place it was lawfully entitled to be, to observe plainly visible happenings, did not run afoul of the Fourth Amendment.").

53. *Leaders of a Beautiful Struggle*, 2 F.4th at 333 ("In August 2016, the public learned for the first time that the BPD was using new aerial technology—planes equipped with high-tech cameras—to surveil Baltimore City. News reports revealed that, several months earlier, BPD partnered with a private contractor based in Ohio, Persistent Surveillance Systems ('PSS'), to conduct aerial surveillance. In the face of public outcry, the program was discontinued.").

billionaire John Arnold, the BPD began piloting the "Aerial Investigation Research" (AIR) program.[54]

The AIR program, approved by a local governmental board for six months, was expected to fly three planes equipped with powerful surveillance cameras over the Baltimore area.[55] The planes could film 90% of the city, covering thirty-two square miles, and could take a photograph every second for twelve hours a day.[56] Video footage was to be kept for forty-five days.[57] The planes only flew during daylight hours and recorded images at a reduced level of granularity, essentially marking objects but not identifying people.[58]

The aerial footage was sent back to ground stations where analysts could use the video images to investigate crimes.[59] So, for example, an analyst could examine the relevant footage of a bank robbery to observe the vehicles driving away from the scene. The data was not analyzed in real time and was limited to the most serious crimes.[60] The analysts would create reports based on the videos that were sent to police and prosecutors.[61] Because the aerial footage only captured location and movement of objects, the analysts would integrate the footage with other surveillance data collected by the police department. Data from automated license plate readers, ground-level cameras, dispatch information, "Shot Spotter sensors," and other details were to be included in the reports sent to investigators.[62]

---

54. Ethan McLeod, *Aerial Surveillance Planes to Begin Flying over Baltimore Friday*, BALT. BUS. J. (Apr. 30, 2020), https://www.bizjournals.com/baltimore/news/2020/04/30/aerial-surveillance-planes-to-begin-flying-over.html. This Article uses PSS and AIR interchangeably. PSS is the company. AIR is the program. But in Baltimore they were the same.

55. *Id.*

56. *Leaders of a Beautiful Struggle*, 2 F.4th at 334 ("The AIR program uses aerial photography to track movements related to serious crimes. Multiple planes fly distinct orbits above Baltimore, equipped with PSS's camera technology known as the 'Hawkeye Wide Area Imaging System.' The cameras capture roughly 32 square miles per image per second. The planes fly at least 40 hours a week, obtaining an estimated twelve hours of coverage of around 90% of the city each day, weather permitting.").

57. *Id.* ("AIR data is stored on PSS's servers, and '[PSS] will retain the AIR imagery data for forty-five days.'" (alteration in original)).

58. *Id.* ("The [Professional Services Agreement (PSA)] limits collection to daylight hours and limits the photographic resolution to one pixel per person or vehicle, though neither restriction is required by the technology. In other words, any single AIR image—captured once per second—includes around 32 square miles of Baltimore and can be magnified to a point where people and cars are individually visible, but only as blurred dots or blobs.").

59. *Id.* ("The planes transmit their photographs to PSS 'ground stations' where contractors use the data to 'track individuals and vehicles from a crime scene and extract information to assist BPD in the investigation of Target Crimes.' 'Target Crimes' are homicides and attempted murder; shootings with injury; armed robbery; and carjacking. Between 15 and 25 PSS contractors analyze the data, working in two shifts per day, seven days per week." (citation omitted)).

60. *Id.* ("The AIR program is not designed to provide real-time analysis when a crime takes place, though.").

61. *Id.* ("[T]he analysts prepare 'reports' and 'briefings' about a Target Crime as requested by the BPD officers on the case. PSS aims to provide an initial briefing within 18 hours and a more in-depth 'Investigation Briefing Report' within 72 hours.").

62. *Id.* ("Further, PSS may 'integrate . . . BPD systems' into its proprietary software 'to help make all of the systems work together to enhance their ability to help solve and deter crimes.' The PSA lists BPD's

The result of the Baltimore PSS-AIR experiment was an almost city-wide visual surveillance system that could be queried for particular investigations.[63] It represented one of the most sophisticated and ambitious targetable surveillance technologies ever designed. Because much of the city was covered, the only limitations were those self-imposed by the police department's own internal policy (e.g., twelve-hour flight duration, daytime hours, forty-five-days retention). No judicial intervention or warrant was required. Observers of the program found that some of those self-imposed limitations were not always followed in practice.[64]

The ACLU and the non-profit group Leaders of a Beautiful Struggle sued to stop the BPD from using PSS planes. The plaintiffs requested a preliminary injunction, claiming irreparable injury under the Fourth and First Amendments.[65] As community activists and critics of the police, Leaders of a Beautiful Struggle asserted that their movements should remain free from the chilling impact of large-scale public surveillance.[66] Because the aerial cameras could track them by location, plaintiffs claimed their reasonable expectation of privacy was violated, making warrantless collection of this information a search for Fourth Amendment purposes.[67] Further, because PSS-AIR was designed to be integrated with other technologies, including audio sensors, ground-level cameras, and automated license plate readers, the tracking systems could be quite revealing of their private lives.[68] The defendant City of Baltimore responded by highlighting the limited nature of the program, the proposed internal accountability measures, and some promised technological limitations, all of which were meant to assuage concerns about the privacy implications.[69]

Part III of this Article will explore the Fourth Circuit's en banc holding that the Baltimore PSS violated the Fourth Amendment. But, for current definitional purposes, the Baltimore pilot project offers one of the clearest examples of a persistent mass surveillance experiment in American history.

---

dispatch system, 'CitiWatch' security cameras, 'Shot Spotter' gunshot detection, and license plate readers as systems to be integrated. As a result, AIR reports may include ground-based images of the surveilled targets from 'the cameras they pass on the way.'" (citation omitted)).

63. *See id.* ("The reports may include, from both before and after the crime: 'observations of driving patterns and driving behaviors'; the 'tracks' of vehicles and people present at the scene; the locations those vehicles and people visited; and, eventually, the tracks of the people whom those people met with and the locations they came from and went to.").

64. *See* Brief of Amici Curiae Electronic Frontier Foundation et al. in Support of Plaintiffs-Appellants' Petition for Rehearing En Banc at 9–10, Leaders of a Beautiful Struggle v. Balt. Police Dep't, 2 F.4th 330 (4th Cir. 2021) (No. 20-1495), 2020 WL 7021614, at *9–10 (describing how some of the limitations in policy were ignored in practice).

65. *See* Brief for Plaintiffs-Appellants at 17, Leaders of a Beautiful Struggle v. Balt. Police Dep't, 2 F.4th 330 (4th Cir. 2021) (No. 20-1495), 2020 WL 2310452, at *17.

66. *Id.* at 3–5.

67. *Id.* at 15–16.

68. *Id.* at 9–12.

69. *See* Brief of Defendants-Appellees at 16–17, Leaders of a Beautiful Struggle v. Balt. Police Dep't, 2 F.4th 330 (4th Cir. 2021) (No. 20-1495), 2020 WL 3089008, at *16–17.

2. Warrantless Long-Term Pole Camera Surveillance

A more familiar form of law enforcement surveillance arose in a case in which the Seventh Circuit upheld the use of a warrantless pole camera system.[70] *United States v. Tuggle* involved a suspected methamphetamine manufacturer and the investigators' choice to set up video cameras around the suspect's home.[71] As the court explained:

> The government installed three cameras on public property that viewed Tuggle's home. Agents mounted two cameras on a pole in an alley next to his residence and a third on a pole one block south of the other two cameras. The first two cameras viewed the front of Tuggle's home and an adjoining parking area. The third camera also viewed the outside of his home but primarily captured a shed owned by Tuggle's coconspirator and codefendant, Joshua Vaultonburg.[72]

Because the cameras faced the suspect's home, all the activities that took place in front of and around the house and all the people entering and exiting the house were recorded.[73] Investigators kept the cameras in place for eighteen months.[74]

The cameras sent the video footage to an FBI office, which allowed the investigators to study what was happening around the home.[75] The cameras allowed for real time and retrospective searching along with panning, tilt, zoom, and low lighting capabilities.[76] Over 100 instances of activity were later used by investigators to build a criminal case against Tuggle.[77] The result of this individualized targeted surveillance was to provide police with a comprehensive video picture of one part of Mr. Tuggle's life and insights about his associations and family activities.

Tuggle challenged the use of the long-term pole camera as a Fourth Amendment violation, arguing that his expectation of privacy to live in his

---

70. United States v. Tuggle, 4 F.4th 505, 510–11 (7th Cir. 2021) ("Tuggle's case presents an issue of first impression for this Court: whether the warrantless use of pole cameras to observe a home on either a short- or long-term basis amounts to a 'search' under the Fourth Amendment.").

71. *Id.* at 511.

72. *Id.*

73. *Id.*

74. *Id.* ("Together, the three cameras captured nearly eighteen months of footage by recording Tuggle's property between 2014 and 2016.").

75. *Id.* ("While officers frequently monitored the live feed during business hours, they could later review all the footage, which the government stored at the Federal Bureau of Investigation office in Springfield, Illinois.").

76. *Id.* ("While in use, the cameras recorded around the clock. Rudimentary lighting technology improved the quality of overnight footage, although the cameras did not have infrared or audio capabilities. Law enforcement agents could also remotely zoom, pan, and tilt the cameras and review the camera footage in real time, though the footage captured only the exterior of Tuggle's house.").

77. *Id.* ("The officers tallied over 100 instances of what they suspected were deliveries of methamphetamine to Tuggle's residence.").

home without government surveillance was infringed.[78] In an openly conflicted-sounding opinion that acknowledged the dangers of big data surveillance,[79] the Seventh Circuit Court of Appeals rejected the Fourth Amendment argument, finding that the court was bound by existing precedent that generally upheld the use of warrantless public pole cameras.[80] As will be discussed in Part II, the court analyzed the cases in a traditional manner but strongly hinted that the Fourth Amendment might need to be reimagined in the face of new, persistent digital surveillance technologies.

C. Is Persistent Surveillance Different?

Is the type of persistent surveillance on display in Baltimore or in *Tuggle* different enough from traditional forms of police surveillance such that it requires a new constitutional analysis? This question is central to this Article and the choices courts must make in addressing Fourth Amendment challenges. Part II will argue that the Supreme Court has implicitly acknowledged a difference in its recent technology cases and that a proper understanding of the interconnected surveillance systems also counsels for a new appreciation of the differences. But at a gut level, judges must grapple with whether continuous monitoring of individuals or places using always-on digital technology is different enough that courts should adopt a different framework for Fourth Amendment analysis.

This is not a new problem. Scholars have attempted to articulate the impacts of privacy-invading surveillance for years now.[81] For example, one way to think about the question of persistent surveillance is to think about the harms it creates. Privacy scholars have forcefully argued that enhanced surveillance

78. Appellant's Brief & Appendix at 4, United States v. Tuggle, 4 F.4th 505 (7th Cir. 2021) (No. 20-2352), 2021 WL 320116, at *4.

79. In *Tuggle*, Judge Flaum addresses his concern with the growing scope of new surveillance technologies and the fear that the current Fourth Amendment doctrine cannot address these privacy and security concerns. *Tuggle*, 4 F.4th at 509–10.

80. *See id.* at 511.

81. The advent of cameras sparked early privacy scholarship around surveillance technologies. *E.g.*, Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 213–14 (1890). For top-level highlights of just a few articles on the subject, see, for example, David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 101–03 (2013); Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309, 1334–36 (2012); James J. Tomkovicz, *Technology and the Threshold of the Fourth Amendment: A Tale of Two Futures*, 72 MISS. L.J. 317, 322–23 (2002).

undermines human values of intimacy,[82] autonomy,[83] association,[84] creativity,[85] obscurity,[86] and, of course, privacy.[87] Legal scholars have cautioned against collective harms,[88] power harms,[89] racial harms,[90] civic harms,[91] and prosecution harms[92] from enhanced government surveillance. Various technological innovations from drones,[93] to the "Internet of Things,"[94] to smart cities[95] have been analyzed with numerous frameworks to examine privacy,[96] secrecy,[97]

82. *See generally* Danielle Keats Citron, *Sexual Privacy*, 128 YALE L.J. 1870, 1908–24 (2018) (discussing risks in exposing sexual intimacy).

83. *See generally* Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1425–26 (2000) (explaining informational autonomy).

84. *See* Katherine J. Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. REV. 741, 761–62 (2008) ("Just as 'dataveillance' can chill an individual's experimentation with particular ideas or pastimes, relational surveillance can chill tentative associations and experimentation with various group identities." (footnote omitted)).

85. *See generally* Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1951–52 (2013) (describing the value of intellectual privacy).

86. *See* Woodrow Hartzog & Evan Selinger, *Surveillance as Loss of Obscurity*, 72 WASH. & LEE L. REV. 1343, 1369 (2015); *see also* Woodrow Hartzog & Evan Selinger, Opinion, *Why You Can No Longer Get Lost in the Crowd*, N.Y. TIMES (Apr. 17, 2019), https://www.nytimes.com/2019/04/17/opinion/data-privacy.html.

87. *See, e.g.*, Julie E. Cohen, *Privacy, Visibility, Transparency, and Exposure*, 75 U. CHI. L. REV. 181, 195–96 (2008); Neil M. Richards, *The Information Privacy Law Project*, 94 GEO. L.J. 1087, 1101–02 (2006) (book review); Paul M. Schwartz & William M. Treanor, *The New Privacy*, 101 MICH. L. REV. 2163, 2177 & n.33 (2003) (book review); Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1093, 1125–29 (2002); A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1463 (2000); Anita L. Allen, *Coercing Privacy*, 40 WM. & MARY L. REV. 723, 738–40 (1999).

88. David Gray, *A Collective Right to Be Secure from Unreasonable Tracking*, 48 TEX. TECH L. REV. 189, 191 (2015).

89. Raymond Shih Ray Ku, *The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance*, 86 MINN. L. REV. 1325, 1326 (2002).

90. BENJAMIN, *supra* note 22, at 112–13; Laura M. Moy, *A Taxonomy of Police Technology's Racial Inequity Problems*, 2021 U. ILL. L. REV. 139, 154.

91. Gray & Citron, *supra* note 81, at 77–78 ("Privacy preserves space for engaging in the critical functions of citizenship. Self-rule requires a 'group-oriented process of critical discourse' among autonomous individuals. The persistent logging of our online activities and offline travels interferes with civic participation and deliberation." (footnotes omitted)).

92. Andrew Guthrie Ferguson, *Big Data Prosecution and* Brady, 67 UCLA L. REV. 180, 206 (2020) (discussing prosecutors' growing reliance on big data surveillance systems and due process implications).

93. Laperruque, *supra* note 44, at 717.

94. Andrew Guthrie Ferguson, *The "Smart" Fourth Amendment*, 102 CORNELL L. REV. 547, 560-61 (2017) (discussing the growth of the Internet of Things, connected devices within the Internet of Things, and the Fourth Amendment).

95. Andrew Guthrie Ferguson, *Structural Sensor Surveillance*, 106 IOWA L. REV. 47, 53 (2020) (discussing whether smart city surveillance violates the Fourth Amendment).

96. Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 496 (2006).

97. Tomkovicz, *supra* note 81, at 341 ("The core value is, in essence, an interest in *secrecy*—in not having the details of our lives learned or exposed against our wishes.").

inequality,[98] and security[99] arising from new surveillance technologies.[100] Entire academic disciplines of surveillance studies now exist to analyze the harms of different forms of consumer and governmental data collection.[101] These scholarly critiques do more than suggest that persistent surveillance is different than traditional surveillance in terms of harmful impact; in fact, they largely confirm the reality. Harm, thus, might be one way to differentiate digital persistent surveillance from traditional police surveillance, but the subject has been well covered by other scholars.

This Part offers a more fundamental insight into the differentiation between traditional surveillance and persistent surveillance—namely how *the act* of persistent surveilling changes the analysis. My argument is that another way to see how always-on, persistent surveillance is distinguishable from traditional surveillance is to look at how the act of monitoring becomes something different because of the non-human, machine technology being used.

More specifically, I argue that all digital persistent surveillance shares six attributes that differentiate what is happening from traditional police surveillance (and the case law developed around that human monitoring). Because all digital persistent surveillance technologies involve increased (1) automation, (2) acceleration, (3) accuracy, (4) accumulation, (5) aggregation, and (6) actualization of data, the resulting surveillance capacity is in fact different from the traditional analog equivalent.[102]

Each of the six alliterative "A" attributes will be discussed to justify the need for the new constitutional analysis to come. Again, if one agrees that there is a cognizable difference between the act of persistently surveilling someone and traditional surveillance, then the argument for a different Fourth Amendment approach grows stronger.

1. Automation

As an initial matter, persistent surveillance should be thought of as a continuous series of automated acts, not a single isolated act.[103] The digital

98. *See generally* Dorothy E. Roberts, *Digitizing the Carceral State*, 132 HARV. L. REV. 1695 (2019) (reviewing VIRGINIA EUBANKS, AUTOMATING INEQUALITY: HOW HIGH-TECH TOOLS PROFILE, POLICE, AND PUNISH THE POOR (2018)); Southerland, *supra* note 22, at 501.

99. Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 104 (2008) ("The Fourth Amendment does not guarantee a right of privacy. It guarantees—if its actual words mean anything—a right of *security*.").

100. WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 34–43 (2018).

101. *See, e.g.*, SURVEILLANCE & SOC'Y, https://ojs.library.queensu.ca/index.php/surveillance-and-society/; *Journal*, SURVEILLANCE STUD. NETWORK, https://www.surveillance-studies.net/?cat=9.

102. *See* Andrew Guthrie Ferguson, *Why Digital Policing is Different*, 83 OHIO ST. L.J. (forthcoming 2022) (detailing why courts analyzing digital surveillance technology should not rely on older, analog Fourth Amendment cases).

103. Meg Leta Jones, *The Ironies of Automation Law: Tying Policy Knots with Fair Automation Practices Principles*, 18 VAND. J. ENT. & TECH. L. 77, 84 (2015) ("Broadly, automation includes all the ways computers

collection technology (be it video, sensors, signals, etc.) is not conducting a single search, but millions of constant searches due to automation.[104] Think of what is happening as the difference between taking a single photograph and a year's worth of videos spliced and saved frame by frame.

Continuous automation creates a more complicated reality for analysis. For example, in a traditional Fourth Amendment case, the act analysis was rather straightforward to apply. First, there was almost always a government agent acting in a specific, singular manner.[105] Perhaps the agents of the Crown invaded an individual's home to search for seditious material.[106] Or, perhaps police placed a bug on a telephone booth to listen to a phone call.[107] Or, maybe police trespassed onto a piece of physical property to investigate.[108] While the Supreme Court did not always agree on how to evaluate the constitutionality of the act, at least the act could be isolated for analysis. It usually was a singular event on a particular day at a particular time and place.

Automation changes the calculus because the government is asking the technology to keep collecting continuously ("persistently"). Continually recording all of an individual's phone calls for months is a different act than capturing a few payphone conversations.[109] Recording all of a city's movements is different than a single flight over a home.[110] Digital automation turns a single search of a home into a series of continual searches of that home. Automation allows all phone calls, or all scans of a home, to be captured with the same ease as just the initial investigative act. In addition, the automated nature results in

---

and machines help people perform tasks more quickly, accurately, and efficiently. The term 'automation' refers to: (1) the mechanization and integration of the sensing of environmental variables through artificial sensors, (2) data processing and decision making by computers, and (3) mechanical action by devices that apply forces on the environment or information action through communication to people of information processed.").

104. Woodrow Hartzog et al., *Inefficiently Automated Law Enforcement*, 2015 MICH. ST. L. REV. 1763, 1779 ("[A]utomated systems are highly efficient, which can reduce the cost of surveillance, analysis, and enforcement to negligible levels per incident. Manual surveillance, analysis, and enforcement require manpower, money, and time. Automation can be centralized, cheap, and virtually instantaneous." (footnote omitted)); *see also* Kevin Werbach, *Sensors and Sensibilities*, 28 CARDOZO L. REV. 2321, 2324 (2007) ("Widespread private deployment of networked sensors is inevitable, because it rests on several powerful technological trends that are unlikely to be reversed. The four primary elements of the pervasive surveillance web are cameras, wireless sensor networks, networked devices incorporating location data, and tools for information sharing and aggregation.").

105. Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 615–16 (2011) (describing how automation complicates the Fourth Amendment calculus traditionally based on human actions, when automated machine collection avoids a human collector).

106. Entick v. Carrington (1765) 95 Eng. Rep. 807 (KB), http://www.bailii.org/ew/cases/EWHC/KB/1765/J98.html.

107. Katz v. United States, 389 U.S. 347, 348 (1967).

108. Oliver v. United States, 466 U.S. 170, 173–74 (1984).

109. Tokson, *supra* note 105, at 600 ("[T]he 'automation rationale,' stands for the proposition that there is no legally relevant difference between disclosure of one's personal information to a third party's automated systems and disclosure to a human being.").

110. *See infra* note 232 (discussing the overflight cases).

overbroad collection because the always-on system necessarily captures more than criminal activities, indiscriminately collecting everything.

2. Acceleration

Second, the time and speed of being able to watch and analyze information is accelerated, exceeding any human parallel.[111] Much of what prevented police from abusing old-fashioned surveillance technologies in the past was that consistent monitoring was too time consuming to be useful.[112] For example, eighteen months of real-time video footage would be quite labor-intensive to review. Similarly, filming a city all day would create an overwhelming and unhelpful dataset. Without the ability to create algorithmic shortcuts, the collected information is largely unusable.[113]

Again, the acceleration of digital persistent surveillance technologies removes traditional, human limitations and enhances police power.[114] Digital pattern matching programs allow for faster searches.[115] Time can be compressed because the digital nature of the information allows for more focused searches for objects, people, patterns, or places.[116] The velocity of accumulated information is only useable because the technology allows an acceleration of processing, which was simply unavailable without powerful computer and machine learning systems.

3. Accumulation

Third, the scale and scope of what can be observed is radically expanded as a result of cheap and powerful digital storage technologies. More and more

111. Gray & Citron, *supra* note 81, at 75 ("Information gathering is faster, cheaper, and more comprehensive than ever before. Whereas information gathered by public and private entities once tended to remain in information silos, it is now seamlessly shared with countless organizations via the Internet." (footnote omitted)).

112. United States v. Jones, 565 U.S. 400, 429 (2012) (Alito, J. concurring).

113. Jones, *supra* note 103, at 85–86 ("Digital automation utilizes elegant algorithms to process piles and piles of data to some end," and "[p]rofessionals are incorporating digital automation to make work more efficient and precise.").

114. Dan L. Burk, *Algorithmic Legal Metrics*, 96 NOTRE DAME. L. REV. 1147, 1156 (2021) ("As the speed and capacity of computational processing is added to surveillance practices, the general populace is increasingly the subject of the widespread, computer-enabled collection, searching, and screening of digital records that [Oscar H.] Gandy famously dubbed the 'panoptic sort.'").

115. Gary T. Marx & Glenn W. Muschert, *Personal Information, Borders, and the New Surveillance Studies*, 3 ANN. REV. L. & SOC. SCI. 375, 380 (2007) ("Among the most salient of the dimensions of the new surveillance are its extension of the senses, low visibility, and lower costs. It tends to be involuntary, remote, strategic, integrated, and automated and to involve multiple forms and sources of data such as numbers, audio, video, and narratives. It provides real-time data flows with attention to systems, networks, and individuals; routinizes surveillance into everyday life; creates immediate links between data collection and action; and emphasizes predicting the future and preventing some forms of it.").

116. STANLEY, *supra* note 31, at 17–21; BRIEFCAM, https://www.briefcam.com/.

individual and collective activities are accumulated and potentially revealed in ever expanding datasets.[117] Building off of the automation and acceleration discussed above, the technologies expand what information is captured creating large, stored datasets about people and places.[118]

The consequence of persistent surveillance is that it grabs an exponential amount of data compared to earlier eras. Accumulating information at this scale presents different privacy harms but is also a different act.[119] What police end up with is a different thing. The dataset is bigger, deeper, broader, richer, and more useful than any single source of traditional police data.[120]

4. Aggregation

In addition to just having more information, the information itself reveals more because of the connections and inferences that can be drawn from the data.[121] This aggregation of personal information is something that could not be done in an earlier era.[122] The ease of digital tracking creates more clues to reveal personal and private matters. Where you go, with whom, what you buy, like, and who you love are all trackable through data.[123] While one point of information will not reveal much, the combined sum of data points reveals

117. Stephen Rushin, *The Legislative Response to Mass Police Surveillance*, 79 BROOK. L. REV. 1, 11 (2013) ("[I]ndiscriminate data collection allows law enforcement to aggregate large amounts of information about a single individual, thereby revealing personal information about habits and behaviors. Five of the justices in *Jones* noted in two separate concurrences that the accumulation of large amounts of data on public movements transforms normal surveillance into a potentially unconstitutional invasion of individual privacy.").

118. Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1089 (2002).

119. Professor Daphna Renan has recognized this changed reality and argued for a more administrative approach to accumulated surveillance datasets. Daphna Renan, *The Fourth Amendment as Administrative Governance*, 68 STAN. L. REV. 1039, 1042 (2016) ("While our Fourth Amendment framework is transactional, then, surveillance is increasingly *programmatic*. Rather than responding to a single investigatory incident, the system of searches is designed en masse. Surveillance is ongoing, and the implications for Fourth Amendment values such as privacy are cumulative. Technology has made it easier than ever to collect, combine, share, and retain massive amounts of data and to search the resulting datasets. The parameters of these surveillance programs—what individuated searches can be run in the datasets, for what purposes, and pursuant to what limitations or protections—are designed through administrative policies." (footnotes omitted)).

120. Sarah Brayne, *The Criminal Law and Law Enforcement Implications of Big Data*, 14 ANN. REV. L. & SOC. SCI. 293, 294 (2018).

121. Solove, *supra* note 96, at 514 ("Aggregation creates . . . a 'digital person,' a portrait composed of information fragments combined together.").

122. Gray & Citron, *supra* note 81, at 75 ("Aggregation technology and advanced statistical analysis tools have enhanced the capacities of those who wield surveillance technology to know us, often in ways that we do not know ourselves.").

123. Susan Freiwald & Stephen Wm. Smith, *The* Carpenter *Chronicle: A Near-Perfect Surveillance*, 132 HARV. L. REV. 205, 221 (2018) (discussing the tracking power of cell site location information technology); *see also* FERGUSON, *supra* note 4 (discussing the rise of police surveillance technologies).

everything.[124] This "mosaic theory" idea arose from the GPS cases but grew in sophistication as digital technologies became more expansive.[125]

Aggregation with large datasets allows police to see patterns of movement, associations, and activities that were not observable before.[126] These digital patterns can expose personal habits involving health, politics, religion, hobbies, or personal connections. The long-term nature of data collection makes such patterns more revealing and potentially more incriminating. It is also just a new capacity that did not exist with siloed, rudimentary surveillance tools.

5. Accuracy

Fifth, digital machines provide a greater level of accuracy compared to humans. As might be obvious, video images can tell a more complete story than a human narrator recounting the same scene.[127] Sensors can provide precise information about location, time, patterns, and other details far more comprehensive than human equivalents.

In addition, the machine that processes the data has none of the inherent limitations of human memory, perception, and attention. One of the most obvious differentiators between traditional surveillance and digital persistent

124. *Cf.* Monu Bedi, *Social Networks, Government Surveillance, and the Fourth Amendment Mosaic Theory*, 94 B.U. L. REV. 1809, 1834 (2014); Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 344 (2012).

125. Matthew B. Kugler & Lior Jacob Strahilevitz, *Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory*, 2015 SUP. CT. REV. 205, 206; *see also* Recent Case, *Criminal Procedure—Fourth Amendment—Seventh Circuit Holds Long-Term, Warrantless Video Surveillance Is Not an Illegal Search.*—United States v. Tuggle*, 4 F.4th 505 (7th Cir. 2021)*, 135 HARV. L. REV. 928, 934–35 (2022) ("Adopting the mosaic theory to limit continuous surveillance would better protect privacy against erosion by a flood of cheap, new monitoring technologies. Privacy violations impose real harms on both individuals and society—harms that are no less serious because they are hard to measure, involve future injury and chilling effects, and can be small but numerous. Mosaic theory recognizes that these small harms accumulate as the amount of surveillance grows.").

126. Andrew Guthrie Ferguson, *Illuminating Black Data Policing*, 15 OHIO ST. J. CRIM. L. 503, 503 (2018) ("Crime, criminals, and patterns of criminal activity will be reduced to data to be studied, crunched, and predicted. Police departments across the United States—like the civilian population—will learn to adapt to ever-shifting technological innovations and efficiencies. The question of adoption is not 'if,' but 'when,' and any delay largely will be a function of money and police culture. The benefits of big data policing involve smarter policing, faster investigation, predictive deterrence, and the ability to visualize crime problems in new ways."); Robert Brauneis & Ellen P. Goodman, *Algorithmic Transparency for the Smart City*, 20 YALE J.L. & TECH. 103, 107 (2018) ("One of the goals is to find patterns in big data sets—for example, the places and times crime is most likely to occur—and to generate predictive models to guide the allocation of public services—for example, how and where to police.").

127. Of course, as we have learned with police-worn body cameras, who possesses the video, how it is analyzed, and who controls the narrative will interfere with accuracy. Video from police-worn body cameras has not provided a more accurate picture of police use of force. While some benefits of transparency exist, large-scale accountability has not followed adoptions of police-controlled video systems. *See, e.g.*, Seth W. Stoughton, *Police Body-Worn Cameras*, 96 N.C. L. REV. 1363, 1421 (2018); Richard E. Myers II, *Police-Generated Digital Video: Five Key Questions, Multiple Audiences, and a Range of Answers*, 96 N.C. L. REV. 1237, 1238 (2018); Mary D. Fan, *Missing Police Body Camera Videos: Remedies, Evidentiary Fairness, and Automatic Activation*, 52 GA. L. REV. 57, 69 (2017).

surveillance, then, is that the latter is far more accurate for some tasks.[128] While computers, object recognition, and other programmable systems often get things wrong when dealing with a vast amount of information, they can outperform humans in matching images or faces or finding particular things. As but one example, even conceding that a facial recognition matching system with billions of images can falsely match two individuals,[129] the same matching task would be almost impossible for a human to accomplish at scale.[130] A human analyst simply could not sort through billions of images with any accuracy.[131] While accuracy is a misleading term—because both computer systems and humans make errors as a routine matter—the ability to match searched-for terms or objects is much easier in digital systems.[132]

6. Actualization

All of this collected data can be actualized because it is converted into digital code and thus made accessible through massive stored systems of collected information. Whereas a non-digital camera system might collect video footage, it might not be as valuable in the ordinary course because there is just too much information (or the data would be siloed and unsearchable).[133] However, with digital coding, information now can be searched across a greater

128. The normative accuracy claim is contestable, but frequently made. *See, e.g.*, Jonathan Turley, *Anonymity, Obscurity, and Technology: Reconsidering Privacy in the Age of Biometrics*, 100 B.U. L. REV. 2179, 2198 (2020) ("Biometric technology represents the marriage of surveillance technology (including some previously available technology) and information technology, allowing for rapid and accurate identification of individuals."); Kristine Hamann & Rachel Smith, *Facial Recognition Technology: Where Will It Take Us?*, CRIM. JUST., Spring 2019, at 9, 9 ("Facial recognition technology provides a sophisticated surveillance technique that can be more accurate than the human eye.").

129. Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROC. MACH. LEARNING RSCH. 77, 87 (2018) ("The most improvement is needed on darker females specifically."); Joy Buolamwini, *When AI Fails on Oprah, Serena Williams, and Michelle Obama, It's Time to Face the Truth*, MEDIUM (July 4, 2018), https://medium.com/@Joy.Buolamwini/when-ai-fails-on-oprah-serena-williams-and-michelle-obama-its-time-to-face-truth-bf7c2c8a4119 ("Error rates were as high as 35% for darker-skinned women . . . .").

130. This is not a normative endorsement of facial recognition. I have extensively explained my position in an earlier Article. *See* Ferguson, *supra* note 40, at 1108. However, under controlled circumstances, the technology does accurately match some faces in ways that could not be done at scale by humans. PATRICK GROTHER ET AL., NAT'L INST. OF STANDARDS & TECH., FACE RECOGNITION VENDOR TEST (FRVT) PART 3: DEMOGRAPHIC EFFECTS 2–3 (2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

131. There is still an open and more fundamental question about whether such an analyst should be given the power to use facial recognition. *See* Hartzog & Selinger, *supra* note 86.

132. Julian Sanchez, *The Pinpoint Search: How Super-Accurate Surveillance Technology Threatens Our Privacy*, REASON (Jan. 10, 2007), https://reason.com/2007/01/10/the-pinpoint-search/.

133. Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. PA. L. REV. 327, 365 (2015) ("To solve crimes, law enforcement must not only collect information, but also identify and link individuals to their accumulated data. In short, data must be connected with identifiable human beings. Facial recognition software, biometric identification technologies, and mobile communication make it easier to identify unknown suspects and access data associated with these suspects.").

set of data systems, allowing for discoveries that were simply impossible even with a large human investigative operation.[134]

Most importantly, investigators can access the information retrospectively—creating a "time machine" to find past events.[135] Being able to use object recognition (or facial recognition) to find a particular thing (or person) from an otherwise overwhelming amount of digital noise is a significant new capacity.[136] In many ways, accessing the collected datasets is the greatest change with new persistent surveillance technologies.[137] Building useful, connected datasets that allow police to access stored information and identify people, places, and problematic activities is what gives big data policing a new (and different) power.

7. Conclusion on Why Persistent Surveillance is Different

The four "V's" of big data differentiation[138]—volume, velocity, variety and veracity are mirrored in the six "A's" discussed above. Simply put, traditional investigatory acts—but persistent and digital—are not really the same thing at all. There is a difference in monitoring something intensely and continuously, compared to monitoring something intensely but episodically or intensely but generally. And this difference has a real effect when one is talking about the government looking for criminal wrongdoing. Police power increases as an individual's ability to value obscurity, autonomy, intimacy, or collective action shrinks. This difference is because the thing of what is happening—digital persistent surveillance—is different than prior analog surveillance technologies (and human observation).

---

134. Joh, *supra* note 37, at 19 ("Big data will revolutionize the surveillance discretion of the police. By allowing the identification of large numbers of suspicious activities and people by sifting through large quantities of digitized data, big data expands the surveillance discretion of the police.").

135. Stephen E. Henderson, *Fourth Amendment Time Machines (and What They Might Say About Police Body Cameras)*, 18 U. PA. J. CONST. L. 933, 935 (2016).

136. Eoin Higgins, *Pre-Crime Policing Is Closer Than You Think, and It's Freaking People Out*, VICE (June 12, 2018, 2:47 PM), https://www.vice.com/en_us/article/7xmmvy/why-does-hartford-have-so-many-cameras-precrime; JOHN S. HOLLYWOOD ET AL., RAND CORP., REAL-TIME CRIME CENTERS IN CHICAGO: EVALUATION OF THE CHICAGO POLICE DEPARTMENT'S STRATEGIC DECISION SUPPORT CENTERS 36, 38 (2019).

137. The focus on accessing stored data as a Fourth Amendment harm has been recognized by scholars. *See, e.g.*, Emily Berman, *When Database Queries Are Fourth Amendment Searches*, 102 MINN. L. REV. 577, 579 (2017) ("I contend that when database queries about particular U.S. persons have the capacity to aggregate data such that it will reveal information that, in the absence of aggregation, the government could only access by conducting a search or seizure, the extraction of that information should be subject to constitutionally based limits.").

138. "Big data can also be defined by four characteristics, referred to as the four V's:

• volume (the growing amount of data);

• velocity (the incredible speed at which data is moving in and out of organizations);

• variety (the wide variety of data types, formats, and sources); and

• veracity (the level of certainty and reliability of data sources)."

Laura Rickett, *Big Data and Risk Assessment*, INTERNAL AUDITING, Sept./Oct. 2016, 2016 WL 6915819.

As will be discussed, this difference in the non-human, digital nature of the act has important legal consequences. With persistent surveillance technologies, the issue is not whether one expects privacy in public from *other people* who could be watching (the basis of traditional expectations of privacy), but whether one expects privacy in public from accurate and automated machines that are constantly watching.[139] The legal and technological analysis necessary to adapt to the challenges of new persistent surveillance technologies is the subject of the next Part.

II. A PERSISTENT SURVEILLANCE FRAMEWORK: LEGAL AND TECHNOLOGICAL QUESTIONS

If persistent surveillance is different, the question then becomes how a constitutional doctrine created for traditional surveillance should be applied. The current answer is somewhat unsatisfying. Courts have not always acknowledged the difference between persistent surveillance and traditional surveillance.[140] Much of the Fourth Amendment doctrine is not only old but old-fashioned, and cases from a pre-Internet and almost pre-digital era still govern police actions.[141]

Current law asks whether a particular police action violated a reasonable expectation of privacy.[142] If so, it is considered a Fourth Amendment search and requires a warrant (absent an exception).[143] The law is decidedly analog, with the famed *Katz* "reasonable expectation of privacy" test arising from a tape recorder being physically taped to a freestanding, coin-operated telephone booth.[144] In fact, a good percentage of Fourth Amendment precedent rests on analogies to now-outdated technologies.[145] It is thus not surprising that as a matter of doctrine and digital relevance, the reasonable expectation of privacy test has been roundly criticized.[146]

---

139. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) ("For that reason, 'society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period.'" (quoting United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring))).

140. For example, the trial court in *Beautiful Struggle* and the trial and appellate courts in *Tuggle* simply applied old analog law to new technologies. *See infra* Part III.

141. As an example, the cell site location information in *Carpenter* was litigated by arguing that the holdings of 1970s cases involving landline telephones and paper bank records should control analysis. *See* Smith v. Maryland, 442 U.S. 735, 744–45; United States v. Miller, 425 U.S. 435, 442 (1976).

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

143. *Id.* at 362.

144. *Id.* at 360; Brief for Petitioner, Katz v. United States, 389 U.S. 347 (1967) (No. 35), 1967 WL 113605, at *5 ("The recorder microphone was taped onto the booth and no part of the microphone physically penetrated the telephone booths.").

145. *See* Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018).

146. Justice Clarence Thomas in his *Carpenter* dissent offers a vehement critique of the *Katz* test, and others have also raised concerns. *Id.* at 2236 (Thomas, J., dissenting) ("The *Katz* test has no basis in the text or history of the Fourth Amendment. And, it invites courts to make judgments about policy, not law. Until

The Supreme Court has hinted that an update may be needed for the Fourth Amendment. In a handful of recent cases, some Justices clearly recognized that "[d]igital is [d]ifferent" when it comes to policing technologies.[147] This Part attempts to offer some clarifying insights about the path forward for the Fourth Amendment based on those cases.

This Part is divided into two Subparts, first discussing the legal questions courts should ask in deciding whether a persistent surveillance technology violates the Fourth Amendment and second discussing the technological questions courts should ask before giving a legal answer. The questions highlighted offer insights about what the Supreme Court has done to suggest a framework for future cases and expose the questions largely ignored in addressing the privacy harms of new surveillance technologies. My argument is that both legal and technological questions must be asked and answered to resolve hard puzzles around persistent surveillance systems.

A. Legal Questions Around Persistent Surveillance

This Part builds upon what I have called my "future-proofing" principles for Fourth Amendment doctrine.[148] In prior works, I have applied similar insights to facial recognition technology[149] and smart city sensor surveillance.[150] These principles also apply to persistent surveillance technologies and might offer courts a way to synthesize the suggestions provided by recent Supreme Court cases.

In this Subpart, I frame the questions courts might ask when confronting persistent surveillance technologies like the Baltimore surveillance planes or the long-term pole cameras. Echoes of the six "A" attributes can be heard,[151] but the analysis is decidedly more legal, arising from insights I have drawn from a careful study of Supreme Court precedent.

Specifically, I suggest questions a court can ask to guide it through the Supreme Court's thicket of modern search cases. The questions are: (1) is the technology at issue digital or analog; (2) does the technology aggregate

---

we confront the problems with this test, *Katz* will continue to distort Fourth Amendment jurisprudence."); *see also* Kyllo v. United States, 533 U.S. 27, 34 (2001) ("The *Katz* test—whether the individual has an expectation of privacy that society is prepared to recognize as reasonable—has often been criticized as circular, and hence subjective and unpredictable."); *see, e.g.*, Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1511 (2010) ("The reasonable expectation of privacy test has led to a contentious jurisprudence that is riddled with inconsistency and incoherence.").

147. Jennifer Stisa Granick, *SCOTUS & Cell Phone Searches: Digital Is Different*, JUST SEC. (June 25, 2014), https://www.justsecurity.org/12219/scotus-cell-phone-searches-digital.

148. *See* Ferguson, *supra* note 40, at 1129–41 (discussing the "future-proofing" theory); *see also* Andrew Guthrie Ferguson, *Future-Proofing the Fourth Amendment*, HARV. L. REV. BLOG (June 25, 2018), https://blog.harvardlawreview.org/future-proofing-the-fourth-amendment.

149. *See* Ferguson, *supra* note 40, at 1141–63.

150. *See* Ferguson, *supra* note 95, at 75–76.

151. *See supra* Subpart I.C.

information or keep it siloed for single use; (3) does the technology allow for retrospective searches, or does the data disappear after collection; (4) does the technology provide police a superpower or merely enhance ordinary human senses; (5) does the technology impact First Amendment associational rights; (6) is the surveillance arbitrarily collecting data from everyone, or is it targeted to a particular suspect; and (7) is the surveillance permeating in nature or particularized to time and location.

The goal in asking these questions is to recognize that the answers provide guidance on whether a particular surveillance technology would be considered a Fourth Amendment search under existing Supreme Court precedent. As will become clear, any answer likely fits along a continuum where hitting some number of these concerns will tip a warrantless surveillance action into a Fourth Amendment search because the police action violates a reasonable expectation of privacy. The task is to offer courts an analytical framework to address hard questions arising from new persistent surveillance technologies.

1. Digital or Analog Technology?

The first question a court should ask in addressing the Fourth Amendment implications of new surveillance technologies is whether the device or system is digital or not. Most modern cases, of course, will involve digital technologies, but the question matters because the Supreme Court has suggested "digital is different" when it comes to Fourth Amendment analysis.[152]

In a series of cases—*Riley v. California*,[153] *Jones v. United States*,[154] and *Carpenter v. United States*[155]—the Supreme Court has ruled that analog precedent may not be appropriate for digital technologies like smartphones, GPS devices, and cell-site signals.[156] For example, in *Riley* —a case involving the warrantless search of a smartphone incident to arrest—the Court specifically distinguished the case

152. Kate Weisburd, *Sentenced to Surveillance: Fourth Amendment Limits on Electronic Monitoring*, 98 N.C. L. REV. 717, 721 (2020) ("The Court has likewise recognized that the concept of a 'reasonable expectation of privacy' for Fourth Amendment purposes must reflect the 'seismic shifts in digital technology' that now allow for 'near perfect surveillance' of digital records that 'hold for many Americans the "privacies of life." 'These efforts reflect a bipartisan consensus that, when it comes to government surveillance of private citizens, 'digital is different.'" (footnotes omitted)); *see also* Henderson, *supra* note 135, at 951 (discussing the "digital is different" thinking of the Supreme Court's recent cases).

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

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

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

156. I have termed this the "anti-equivalence principle." *See* Ferguson, *supra* note 40, at 1132–33 ("The Supreme Court's recent cases involving police surveillance have caused a reexamination of existing precedent crafted in a pre-technological age. In its recent technologically-enhanced surveillance cases, the Supreme Court has recognized that digital police capabilities are simply not the equivalent of traditional analog policing methods." (footnotes omitted)).

from its analog precedent.[157] Instead of treating the smartphone like a physical wallet or cigarette pack, recovered incident to arrest,[158] Chief Justice Roberts recognized the qualitative and quantitative differences in scale of digital information existing in a smart device.[159] The privacy harm in terms of scale, scope, time, and quantity was just too great to apply the traditional rules of a search incident to arrest.[160] The revealing and personal data we keep in our smartphones simply has no convincing analog comparison, so equating past police searches with digital searches is misleading and insufficiently protective of privacy.

Similarly, in *Jones*, five concurring Justices recognized that the digital capacity of a single GPS tracking device should not be equated with traditional analog investigative techniques like beepers, even if they might ultimately capture the same tracking information.[161] In what was originally called the mosaic theory,[162] the concurring Justices acknowledged the truth that long-term location data reveals more than the sum of its parts.[163] The digital nature of long-term monitoring was more privacy invasive than the same practice accomplished with physically present human officers.[164]

Finally, the Court in *Carpenter* explicitly cautioned against a "mechanical application" of analog third-party record principles in a world where most things involved data stored by third parties.[165] Whereas cases from the 1970s allowed police access to third-party records of banks and telephone companies

157. *Riley*, 573 U.S. at 386 ("But while *Robinson*'s categorical rule strikes the appropriate balance in the context of physical objects, neither of its rationales has much force with respect to digital content on cell phones.").

158. *Id.* at 400 ("[T]he fact that a search in the pre-digital era could have turned up a photograph or two in a wallet does not justify a search of thousands of photos in a digital gallery.").

159. *Id.* at 393 ("Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person. The term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.").

160. *See id.* at 386 ("A search of the information on a cell phone bears little resemblance to the type of brief physical search considered in [prior precedent].").

161. United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring).

162. United States v. Maynard, 615 F.3d 544, 562 (2010), *aff'd sub nom* United States v. Jones, 565 U.S. 400 (2012).

163. *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring).

164. *Id.* ("I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."); *id.* at 430 (Alito, J., concurring) ("[S]ociety's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period. In this case, for four weeks, law enforcement agents tracked every movement that respondent made in the vehicle he was driving. We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark.").

165. Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) ("[W]e rejected in *Kyllo* a 'mechanical interpretation' of the Fourth Amendment . . . ." (quoting Kyllo v. United States, 533 U.S. 27, 35 (2001))).

without a warrant (under the third-party doctrine),[166] the digital revolution made such access much more privacy invasive.[167] Again, the digital nature of the information at issue pushed the Court to distinguish prior precedent that might have allowed access to cell site location information (CSLI) records without a warrant.[168]

While it would be overstating things to say that the Supreme Court has drawn a bright line between digital search cases and older analog Fourth Amendment cases, it is clear that the distinction matters.[169] Digital surveillance cases have rightly been considered different because of the greater capacity to undermine privacy.[170] This has been a theme of the Court since the advent of new surveillance technologies[171] and should be given greater weight as new police tools develop into systems of surveillance.[172]

Thus, a court facing a Fourth Amendment challenge to a new persistent surveillance technology should initially flag the reality that the digital capacity of the technology might distinguish it from past analog precedent.[173] What might once have been acceptable warrantless collection might not be considered permissible by a court applying a "digital is different" rationale.

2. Aggregated or Single-Use Information?

The second question a court should ask in considering the Fourth Amendment implications of persistent surveillance technologies is about the aggregated nature of the collected information.[174] In *Riley*, *Jones*, and *Carpenter*, the Supreme Court explicitly recognized the privacy harm of aggregating personal data as a distinct (and distinguishable) form of Fourth Amendment

166. *Id.* at 2216.

167. *Id.* at 2219 ("[T]here is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers.").

168. Evan Caminker, *Location Tracking and Digital Data: Can* Carpenter *Build a Stable Privacy Doctrine?*, 2018 SUP. CT. REV. 411, 415 ("*Carpenter* means that a majority of the Justices are searching to find ways to better protect privacy in the modern age. And by retooling long-standing precedent to be more adaptive to privacy concerns . . . .").

169. *Carpenter*, 138 S. Ct. at 2222 ("When confronting new concerns wrought by digital technology, this Court has been careful not to uncritically extend existing precedents.").

170. As the majority stated in *Carpenter*, "[T]he rule the Court adopts 'must take account of more sophisticated systems that are already in use or in development.'" *Id.* at 2218 (quoting *Kyllo*, 533 U.S. at 36).

171. *Kyllo*, 533 U.S. at 36 ("While the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development.").

172. *Carpenter*, 138 S. Ct. at 2214 ("We have kept this attention to Founding-era understandings in mind when applying the Fourth Amendment to innovations in surveillance tools. As technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes, this Court has sought to 'assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'" (alteration in original) (quoting *Kyllo*, 533 U.S. at 34)).

173. *See* Ferguson, *supra* note 102.

174. Again, aggregation as a legal harm to personal privacy is a different concept than aggregation as a technical matter, although both involve connecting the dots about different types of information.

harm.[175] In contrast to early cases involving single-use technologies (such as a tape recording or a beeper), any system that is collecting different types of data or from different times which can be linked together might run into this aggregation issue.[176]

For example, the Court in *Riley* was explicit in recognizing the privacy harm of revealing all of the data in our smartphones.[177] While each piece of information (a phone number, contact, app, or location) itself might not be revealing, put together, the aggregated information created a full picture of the individual's likes, dislikes, and connections.[178] The concurring Justices in *Jones*[179] and the majority in *Carpenter*[180] acknowledged the same insight with location data aggregation. Where we go in the world reveals what we do and in many ways who we are. A single location might not reveal much, but the long-term aggregated information from GPS or CSLI reveals a picture of our interests and activities. Such aggregated information collected by law enforcement without a warrant creates a quantifiably different privacy harm than anything that happened in the analog-policing era.[181]

---

175. *See, e.g.*, Riley v. California, 573 U.S. 373, 394 ("The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet."); United States v. Jones, 565 U.S. 400, 416 (2012) ("I would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements. I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."); *Carpenter*, 138 S. Ct. at 2217 ("Mapping a cell phone's location over the course of 127 days provides an all-encompassing record of the holder's whereabouts. As with GPS information, the time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'" (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J. concurring))).

176. Shaun B. Spencer, *The Aggregation Principle and the Future of Fourth Amendment Jurisprudence*, 41 NEW ENG. J. ON CRIM. & CIV. CONFINEMENT 289, 289 (2015) ("Data aggregation has played a role in three recent cases implicating one's reasonable expectation of privacy under the Fourth Amendment. Although the cases involve disparate doctrines, they all focus on aggregation as a reason to depart from prior law." (footnote omitted)).

177. *Riley,* 573 U.S. at 394–95 ("The storage capacity of cell phones has several interrelated consequences for privacy. First, a cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows even just one type of information to convey far more than previously possible. . . . Third, the data on a phone can date back to the purchase of the phone, or even earlier. A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a phone.").

178. *Id.* at 396–97 ("Indeed, a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.").

179. *Jones*, 565 U.S. at 413–16 (Sotomayor, J., concurring); *id.* at 429–31 (Alito, J., concurring).

180. *Carpenter*, 138 S. Ct. at 2225.

181. Gray & Citron, *supra* note 81, at 101 (theorizing that aggregation of data should factor into a new Fourth Amendment analysis focused in part on quantitative privacy: "In our view, the threshold Fourth Amendment question raised by quantitative privacy concerns is whether an investigative technique or

The distinction between aggregated collection, which raises Fourth Amendment privacy concerns, and single-use, single-source information, which does not, offers another distinguishing line that might guide courts thinking through new surveillance technologies.[182] The more pieces of data collected and the more revealing those pieces are about a person's life, then the more likely the surveillance technology would raise Fourth Amendment concerns. In contrast, the more limited the collection and the more siloed the content, the more likely it is that the technology would survive Fourth Amendment scrutiny.

3. Retrospective or Ephemeral Capabilities?

As discussed, one of the revolutionary changes of digital surveillance technologies is the fact that data can be stored and searched with ease.[183] Surveillance systems do not simply capture video or location data, but allow police to search through the collected information in ways that could not have been done before.[184] A face can be found in a crowd captured among hundreds of hours of video footage.[185] A location of a particular person's cell phone can be found among all the other millions of phones in use.[186] The retrospective nature of recorded digital systems separates out previous technologies where the face or location data might just have disappeared with the passage of time.

Again, as a constitutional matter, *Riley*, *Jones*, and *Carpenter* all acknowledge the danger of giving police a time-machine-like[187] search capability to go back and investigate crime. Stored data allows police to do things they could never do in real time or with traditional capabilities. Justice Sotomayor, in *Jones*, talked about this mining of data trails as a newfound search power.[188] Chief Justice Roberts echoed this concern in *Carpenter*:

---

technology has the capacity to facilitate broad programs of indiscriminate surveillance that raise the specter of a surveillance state if deployment and use of that technology is left to the unfettered discretion of government.").

182. Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1140 (2002); Kerr, *supra* note 124, at 314.

183. *See* Burk, *supra* note 114, at 1156.

184. Of course, the digital feeds need not be set up to collect and store data, but in most cases, the systems are set up to provide later access to the collected information.

185. This technology has not yet been deployed in the United States at any scale. *But see* Simon Denyer, *China's Watchful Eye: Beijing Bets on Facial Recognition in a Big Drive for Total Surveillance*, WASH. POST (Jan. 7, 2018), https://www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance.

186. Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018) ("[B]ecause location information is continually logged for all of the 400 million devices in the United States—not just those belonging to persons who might happen to come under investigation—this newfound tracking capacity runs against everyone.").

187. *See* Henderson, *supra* note 135, at 939.

188. United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) ("The government can store such records and efficiently mine them for information years into the future." (citing United States v. Pineda-Moreno, 617 F.3d 1120, 1124 (9th Cir. 2010) (Kozinski, C.J., dissenting)); *see also Carpenter*, 138 S. Ct. at 2218.

> Moreover, the retrospective quality of the data here gives police access to a category of information otherwise unknowable. In the past, attempts to reconstruct a person's movements were limited by a dearth of records and the frailties of recollection. With access to CSLI, the Government can now travel back in time to retrace a person's whereabouts, subject only to the retention [policies] of the wireless carriers, which currently maintain records for up to five years.[189]

Retrospective CSLI data of course is not the only concern. Almost everything in the digital world (information about financial transactions, Internet searches, apps, medical history, etc.) can be stored and reexamined in ways that raise privacy risks. The ability to capture and search such collections of stored data offers a distinguishing feature for persistent surveillance capabilities.

As a result, courts examining the Fourth Amendment implications of new surveillance technologies thus should ask whether the digital capture of information gives police some new form of retrospective search power. Retrospective searches without a warrant give police an ability to surveil lives and patterns with no external oversight or limits and run right at the heart of the Supreme Court's concerns in *Carpenter* and *Jones*.

4. Superpower or Enhancement?

Another question courts should ask involves whether the surveillance technology gives police an enhancement or a superpower.[190] Generally, the Supreme Court has blessed simple technological enhancements of ordinary human senses[191] but has drawn the line when technologies replace human abilities.[192] Persistent surveillance technologies can provide a bit of both types of extra-sensory surveillance.

---

189. *Carpenter*, 138 S. Ct. at 2218.

190. *See generally*, David A. Harris, *Superman's X-Ray Vision and the Fourth Amendment: The New Gun Detection Technology*, 69 TEMP. L. REV. 1 (1996).

191. Dow Chem. Co. v. United States, 476 U.S. 227, 238 (1986) ("The mere fact that human vision is enhanced somewhat, at least to the degree here, does not give rise to constitutional problems."). This statement in *Dow* is not without qualification as many of the early technology and surveillance cases did not provide more information than ordinary human senses. *Dow* is an outlier in the cases, in that it truly did allow for superhuman surveillance capabilities (albeit focused on commercial industry, not personal homes or property). *See* Ferguson, *supra* note 102.

192. There is some ambiguity about how the Court would treat machine-collected information that is never provided to human investigators. In almost all criminal prosecutions, a human investigator would access or obtain the information. According to some scholars, no Fourth Amendment search occurs until a human gains access to the information. *See, e.g.*, Jones, *supra* note 103, at 94 ("No 'search' by government agents necessarily occurs until information is exposed to a human being. In other words, a human is required to be in the loop for a search to have been performed, meaning a machine alone cannot violate one's right to privacy."); Tokson, *supra* note 105, at 615 ("In cases involving new technologies, the Court's holdings support the idea that no Fourth Amendment 'search' occurs until electronic information is exposed to a human being.").

The easiest example of this line comes from the old-fashioned beeper-tracking cases of *United States v. Knotts*[193] and *United States v. Karo*.[194] In *Knotts*, police agents placed a beeper in a container of chemicals used to manufacture illegal narcotics and followed the beeper to recover evidence.[195] Essentially, the beeper allowed the investigating officers to follow the suspects more efficiently through public roads. The Supreme Court held that there was no Fourth Amendment search because all the beeper did was enhance ordinary visual surveillance normally conducted by law enforcement officers.[196] In contrast, the *Karo* court found a beeper placed in a container of chemicals (also used for illegal drug production) to be a Fourth Amendment search because the beeper revealed the location of a container in a house that could not be observed by ordinary human senses.[197] As the Court recognized, the beeper provided information that could not be observed or obtained without special (x-ray-like) powers.[198] The concurrences in *Jones* echoed this reasoning, recognizing that while technically a team of agents could have surveilled Antoine Jones twenty-four-seven for twenty-eight days, in reality the GPS device was not enhancing human surveillance but offering a completely different power.[199] It was, in essence, a superpower that did more than augment ordinary human capabilities.

Similar lines can be drawn if you contrast *Kyllo*'s ban on a thermal imaging device that can detect heat in a home (which could not be seen with the naked eye) and the overflight cases (*Ciraolo* and *Riley*), which emphasized that the investigating officers were using their ordinary visual senses to see the marijuana growing in the home (albeit from the atypical enhanced position of a police airplane/helicopter).[200] Superpowers that offer police the ability to circumvent

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

194. United States v. Karo, 468 U.S. 705 (1984).

195. *Knotts*, 460 U.S. at 278.

196. As the *Karo* Court interpreted *Knotts*, "The Court held that since the movements of the automobile and the arrival of the can containing the beeper in the area of the cabin could have been observed by the naked eye, no Fourth Amendment violation was committed by monitoring the beeper during the trip to the cabin." *Karo*, 468 U.S. at 713–14.

197. *Id.* at 715 ("The monitoring of an electronic device such as a beeper is, of course, less intrusive than a full-scale search, but it does reveal 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.").

198. *Id.* ("[H]ere, . . . the monitoring indicated that the beeper was inside the house, a fact that could not have been visually verified.").

199. United States v. Jones, 565 U.S. 400, 429 (2012) (Alito, J., concurring) ("In the precomputer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken. The surveillance at issue in this case—constant monitoring of the location of a vehicle for four weeks—would have required a large team of agents, multiple vehicles, and perhaps aerial assistance.").

200. *Compare* Dow Chem. Co. v. United States, 476 U.S. 227, 239 (1986) ("An electronic device to penetrate walls or windows so as to hear and record confidential discussions of chemical formulae or other trade secrets would raise very different and far more serious questions; other protections such as trade secret laws are available to protect commercial activities from private surveillance by competitors."), *with* Kyllo v. United States, 533 U.S. 27, 33 (2001) ("The present case involves officers on a public street engaged in more than naked-eye surveillance of a home. We have previously reserved judgment as to how much technological enhancement of ordinary perception from such a vantage point, if any, is too much. While we upheld

natural human privacy barriers are considered searches (like seeing and hearing through walls), whereas technological enhancements of human senses (flashlights and telescopes) fall outside of Fourth Amendment search scrutiny.[201]

For courts evaluating persistent surveillance technologies, a hard question will be whether the technology enhances or supercharges police power.[202] Some persistent surveillance technologies fall decidedly on the superpower side of the line.[203] Arguably, audio sensors that can hear any gunshot in the city are a superpower (super hearing), and video systems that can simultaneously record the entire city and play back video clips are a superpower (super sight). The fact that these technologies give police superpowers does not mean they are necessarily Fourth Amendment violations but does help separate out the technologies that warrant additional scrutiny.

5. Impacting Associational Freedoms or Not?

The Fourth Amendment was a constitutional hedge against tyranny.[204] In colonial America, arbitrary searches and seizures had been used as political weapons to stifle dissent, and the Founders wanted to create zones of private and associational liberty to resist future tyrannical aspirations.[205] Associational

---

enhanced aerial photography of an industrial complex in *Dow Chemical*, we noted that we found 'it important that this is *not* an area immediately adjacent to a private home, where privacy expectations are most heightened.'" (quoting *Dow Chem. Co.*, 476 U.S. at 237 n.4)).

201. *See, e.g.*, Texas v. Brown, 460 U.S. 730, 738–40 (1983); On Lee v. United States, 343 U.S. 747, 754 (1952) ("The use of bifocals, field glasses or the telescope to magnify the object of a witness' vision is not a forbidden search or seizure, even if they focus without his knowledge or consent upon what one supposes to be private indiscretions.").

202. *Cf.* Burk, *supra* note 114, at 1156 ("Surveillance, sorting, and processing capabilities reinforce and feed on one another. The torrent of available data can only be processed by superhuman, automated means, and in turn the availability of such automated systems invites the continued collection of surveillant data.").

203. Most superheroes would likely be walking Fourth Amendment violations. *See, e.g.*, Superman (x-ray vision would violate *Kyllo*, and super hearing inside of private spaces would violate *Katz*).

204. *See* TIMOTHY SNYDER, ON TYRANNY: TWENTY LESSONS FROM THE TWENTIETH CENTURY 10 (2017) ("[T]he Founding Fathers sought to avoid the evil that they, like the ancient philosophers, called *tyranny*. They had in mind the usurpation of power by a single individual or group, or the circumvention of law by rulers for their own benefit."); *see also, e.g.*, United States v. Zemlyansky, 945 F. Supp. 2d 438, 452 (S.D.N.Y. 2013) ("The Fourth Amendment requires that warrants state with particularity the items to be searched and seized. This requirement traces directly back to the Framers' experience of tyranny before this Nation's founding . . . ."); United States v. Browning, 634 F. Supp. 1101, 1102 (W.D. Tex. 1986) ("The Fourth Amendment of the United States Constitution was written to protect Americans from government tyranny."). *See generally* Andrew Guthrie Ferguson, *Surveillance and the Tyrant Test*, 110 GEO. L.J. 205, 265 (2021) (discussing tyranny and Fourth Amendment protections).

205. James J. Tomkovicz, California v. Acevedo*: The Walls Close in on the Warrant Requirement*, 29 AM. CRIM. L. REV. 1103, 1134 (1992) ("The Framers objected to general warrants and writs of assistance because they resulted in arbitrary deprivations of privacy, property, and liberty. Those deprivations were arbitrary in part because officers were authorized to search and seize upon bare suspicion. They were also arbitrary and dangerous because agents of the executive were given 'unlimited discretion' to choose whom, where, and what to search and seize." (footnotes omitted)).

freedoms, while finding explicit protection in the First Amendment, were also connected to Fourth Amendment history.[206]

Surveillance technologies that potentially impede associational freedoms have been challenged with greater urgency than other more crime-focused technologies.[207] A clear example of this First and Fourth Amendment connection comes from the concurrences in *Jones*, which used the threat of long-term GPS tracking to make an argument about associational liberty:

> Awareness that the government may be watching chills associational and expressive freedoms. And the government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the government, in its unfettered discretion, chooses to track—may "alter the relationship between citizen and government in a way that is inimical to democratic society."[208]

This insight about the intersection of First and Fourth Amendment rights was incorporated into the majority's decision in *Carpenter* with Chief Justice Roberts writing about how cell-site location tracking creates a "detailed, encyclopedic, and effortlessly compiled" record of activities which would include personal and political associations.[209] The Chief Justice recognized, "As with GPS information, the time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'"[210] Surveillance of those associational freedoms thus deserved extra scrutiny.

Again, this associational liberty issue also arose in *Riley*, where the Supreme Court recognized how smartphones reveal political allegiances and policy preferences.[211] The collected contacts, data, and apps on smartphones are not

---

206. Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112, 133 (2007).

207. *See* Riley v. California, 573 U.S. 373, 395–96 (2014).

208. United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring), *vacated*, 565 U.S. 1189 (2012)).

209. Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018) ("The question we confront today is how to apply the Fourth Amendment to a new phenomenon: the ability to chronicle a person's past movements through the record of his cell phone signals. Such tracking partakes of many of the qualities of the GPS monitoring we considered in *Jones*. Much like GPS tracking of a vehicle, cell phone location information is detailed, encyclopedic, and effortlessly compiled.").

210. *Id.* at 2217 (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)); *see id.* at 2217–18 ("In fact, historical cell-site records present even greater privacy concerns than the GPS monitoring of a vehicle we considered in *Jones*.").

211. *Riley*, 573 U.S. at 396 ("Mobile application software on a cell phone, or 'apps,' offer a range of tools for managing detailed information about all aspects of a person's life. There are apps for Democratic Party news and Republican Party news; apps for alcohol, drug, and gambling addictions; apps for sharing prayer requests; apps for tracking pregnancy symptoms; apps for planning your budget; apps for every conceivable hobby or pastime; apps for improving your romantic life.").

just mechanisms of associational communication (using the device to connect) but also revealing of the identity and interests of individuals (detailing preferred news sources and political engagement). In addition, all of the emails, notes, and other work product located on smartphones provide a wealth of information about political association and activism.[212]

Warrantless invasion of this kind of associational information, thus, should be an issue for courts addressing the constitutionality of new surveillance technologies. Those technologies that infringe on associational liberty are to be viewed with extra caution, as they impact First and Fourth Amendment rights. Those technologies that avoid impacting associational liberties will fare better under Fourth Amendment scrutiny.

6. Arbitrary or Targeted Collection?

Courts evaluating persistent surveillance technologies must also consider arbitrariness. A consistent theme in Fourth Amendment cases has been a concern about arbitrary police powers.[213] Surveillance technologies offer police additional powers that can be equally arbitrary, so it is not surprising that the Supreme Court raised concerns about warrantless abuses.[214] Suspicion-less mass surveillance offers an example of how "arbitrariness" suggests a line to mark constitutional from unconstitutional surveillance.

While the *Carpenter* case was nominally focused on Timothy Carpenter's individual Fourth Amendment rights, the Supreme Court did not hide its concern with the potential arbitrary use of warrantless CSLI searches against everyone.[215] As the Court wrote, "Critically, because location information is continually logged for all of the 400 million devices in the United States—not just those belonging to persons who might happen to come under investigation—this newfound tracking capacity runs against everyone."[216] A national network of CSLI data covering just about everyone gave police too

212. Unfortunately, surveillance of political dissenters and racial justice activists has a long history in America. *See, e.g.*, David J. Garrow, *The FBI and Martin Luther King*, ATLANTIC (July/Aug. 2002), https://www.theatlantic.com/magazine/archive/2002/07/the-fbi-and-martin-luther-king/302537/; George Joseph, *Exclusive: Feds Regularly Monitored Black Lives Matter Since Ferguson,* INTERCEPT (July 24, 2015, 1:50 PM), https://theintercept.com/2015/07/24/documents-show-department-homeland-security-monitoring-black-lives-matter-since-ferguson/.

213. *See, e.g.*, Florida v. Riley, 488 U.S. 445, 462 (1989) (Brennan, J., dissenting) ("The basic purpose of this Amendment, as recognized in countless decisions of this Court, is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials." (quoting Camara v. Mun. Ct., 387 U.S. 523, 528 (1967))); INS v. Delgado, 466 U.S. 210, 215 (1984) ("The Fourth Amendment does not proscribe all contact between the police and citizens, but is designed 'to prevent arbitrary and oppressive interference by enforcement officials with the privacy and personal security of individuals.'" (quoting United States v. Martinez-Fuerte, 428 U.S. 543, 554 (1976))).

214. *See Carpenter*, 138 S. Ct. at 2213.

215. *See id.* at 2218.

216. *Id.*

much power that could be too easily abused. The potential arbitrariness of warrantless (and really suspicion-less) searches proved too troubling to withstand Fourth Amendment scrutiny.[217]

The language of arbitrariness also appeared in concerns about GPS tracking by police in *Jones*.[218] The government's argument on appeal had been that police did not need a warrant to track anyone.[219] As Justice Sotomayor stated in her *Jones* concurrence, "[T]he Fourth Amendment's goal [is] to curb *arbitrary* exercises of police power . . . ."[220] Requiring individualized suspicion and a warrant provided a check on that potential arbitrary misuse.

The Supreme Court's modern concern—echoing the Founders' concerns—was that government could use state power to target anyone (and everyone) without a basis in law.[221] Without suspicion, probable cause, a warrant, or legal justification, police could abuse existing power to target individuals or disfavored groups.[222] Again, from *Carpenter*, Chief Justice Roberts emphasized: "'The 'basic purpose of [the Fourth] Amendment,' our cases have recognized, 'is to safeguard the privacy and security of individuals against *arbitrary* invasions by governmental officials.'"[223]

Courts evaluating new surveillance technologies should thus ask whether the technology offers the equivalent of a general warrant power to arbitrarily rummage through personal data. Any technology that runs against a broad group of people may be constitutionally suspect.

7. Permeating or Cabined Surveillance?

The final legal question courts must ask themselves is whether the surveillance system is permeating. In *Carpenter* and *Jones*, the Supreme Court repeated the same somewhat cryptic line that the Fourth Amendment was

---

217. *Id.* at 2214 ("On this score, our cases have recognized some basic guideposts. First, that the Amendment seeks to secure 'the privacies of life' against '*arbitrary* power.'" (emphasis added) (quoting Boyd v. United States, 116 U.S. 616, 630 (1886))).

218. *See* United States v. Jones, 565 U.S. 400, 416–17 (2012) (Sotomayor, J., concurring).

219. *See id.* at 406.

220. *Id.* at 416 (emphasis added).

221. Thomas K. Clancy, *What Does the Fourth Amendment Protect: Property, Privacy, or Security?*, 33 WAKE FOREST L. REV. 307, 309 (1998) ("The Fourth Amendment was a creature of the eighteenth century's strong concern for the protection of real and personal property rights against arbitrary and general searches and seizures.").

222. *See, e.g.*, United States v. Ortiz, 422 U.S. 891, 895 (1975) ("[T]he central concern of the Fourth Amendment is to protect liberty and privacy from arbitrary and oppressive interference by government officials."); Schneckloth v. Bustamonte, 412 U.S. 218, 242 (1973) ("[T]he Fourth Amendment protects the 'security of one's privacy against arbitrary intrusion by the police . . . .'" (quoting Wolf v. Colorado, 338 U.S. 25, 27 (1949), *overruled by* Mapp v. Ohio, 367 U.S. 643 (1961))).

223. Carpenter v. United States, 138 S. Ct. 2206, 2213 (emphasis added) (quoting Camara v. Mun. Ct., 387 U.S. 523, 528 (1967)).

concerned with limiting "too permeating police surveillance."[224] Specifically, in *Carpenter*, the Court stated, "[A] central aim of the Framers was 'to place obstacles in the way of a too permeating police surveillance.'"[225] In *Jones*, Justice Sotomayor stated that "the Fourth Amendment's goal [is] to . . . prevent 'a too permeating police surveillance.'"[226] The language itself comes from *United States v. Di Re*—a case involving a traffic stop and search incident to arrest that was decidedly analog and did not involve surveillance technology or broad search powers.[227]

While the phrase "too permeating surveillance" is admittedly inexact, at least as seen in the CSLI and GPS context, it likely means identifying systems of surveillance that pervade an area or group of people in ways that upset a traditional understanding of government power. The cell network that can identify your phone out of millions offers a permeating surveillance capacity. Satellite GPS tracking that can identify an object for months on end suggests a structural surveillance power that is fixed and inescapable.[228] The key is the scope, scale, and capacity of the established systems that can be used to target groups of people over large areas or timeframes. Certainly, city-wide networks of embedded technologies suggest concerns about permeating surveillance.

In many ways, this "permeating" or "pervasive" or "persistent" quality of new surveillance technologies offers a clarifying distinction from traditional surveillance technologies.[229] As discussed in Part I, the "always on" nature of monitoring, coupled with the intent to find bad acts, fundamentally reshapes the power balance between citizens and the police. Continuous monitoring with the intent to find wrongdoing flips the liberty-focused, or negative-liberties, protection of the Constitution. Instead of living free with only occasional intrusions when there exists particularized reason to suspect an individual of a crime, the technologies allow continuous monitoring of everyone (innocent and guilty). Such a surveillance power clearly disempowers individuals and erodes

224. *Id.* at 2214 (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)); *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring) (quoting *Di Re*, 332 U.S. at 595).

225. *Carpenter*, 138 S. Ct. at 2214 (quoting *Di Re*, 332 U.S. at 595).

226. *Jones*, 565 U.S. at 416–17 (Sotomayor, J., concurring) (quoting *Di Re*, 332 U.S. at 595).

227. *Di Re*, 332 U.S. at 595 ("But the forefathers, after consulting the lessons of history, designed our Constitution to place obstacles in the way of a too permeating police surveillance, which they seemed to think was a greater danger to a free people than the escape of some criminals from punishment.").

228. In fact, such structural, twenty-four-hours-a-day dragnet surveillance was specifically identified as a concern as far back as *Knotts*. United States v. Knotts, 460 U.S. 276, 283–84 (1983) ("Respondent does not actually quarrel with this analysis, though he expresses the generalized view that the result of the holding sought by the Government would be that 'twenty-four hour surveillance of any citizen of this country will be possible, without judicial knowledge or supervision.' . . . [I]f such dragnet-type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable.").

229. One could also add "panvasive" to the pantheon of concerning "p" terms. *See generally* Christopher Slobogin, *Panvasive Surveillance, Political Process Theory, and the Nondelegation Doctrine*, 102 GEO. L.J. 1721 (2014) (discussing panvasive surveillance).

autonomy and liberty interests of those who wish to live without government monitoring.

Courts evaluating a new technology must look at the permeating nature of the system to evaluate its impact. Cabined technologies that focus on particularized places or are limited to particularized moments might evade Fourth Amendment scrutiny, but those technologies that become a fixed source of surveillance power may be challenged.

8. Conclusion About the Legal Analysis Around Persistent Surveillance

The above legal analysis attempts to draw together the threads of how the Supreme Court has examined recent digital surveillance technologies. Certain recurring principles emerge, but how they result in a coherent Fourth Amendment doctrine is far less clear. As will be discussed in Part III, at some point along the continuum of surveillance, the Court will find an invasion of a reasonable expectation of privacy, and thus a search for Fourth Amendment purposes. Where that point exists as a constitutional matter, or how one could recognize it, *ex ante*, is left unexplained, but the framework for analysis exists.

What does seem clear is that the growth of systems of persistent surveillance which allow for targeted investigation through access to large-scale, retrospective datasets creates judiciable Fourth Amendment issues. The Supreme Court appears to be drawing a line at broad and deep digital surveillance systems, which give police access to personal information without a warrant.

This insight highlights the importance of defining the surveillance system at issue. Courts must now grapple with the systems nature of the technology, itself. As discussed in the next Subpart, before applying Fourth Amendment principles to policing technology, courts must figure out what the technology "is" that is doing the surveilling.

B. Technological Questions Around Persistent Surveillance

Courts facing Fourth Amendment challenges to new, persistent surveillance must inquire about the nature of the technology in use. After all, courts cannot answer the legal questions raised above without understanding the scope, scale, and capacity of the technology being analyzed. Therefore, underneath the courts' Fourth Amendment determinations should be equally important considerations (choices, really) involving what they see as the "technology" at issue. Yet, these definitional questions have been largely ignored. This Subpart unearths what I think might be the most important issue to solve the persistent surveillance puzzle—namely how to define the unit of surveillance.

Two separate definitional questions emerge. First, should the technology be thought of as a specific tool or a wider system of surveillance? For example, is a camera just a camera, or do we need to consider the system's integrated search function and how police have incorporated other intersecting data streams into a large-scale database of collected information? Second, in a world of constantly evolving technology, should courts be considering future data collection concerns or just the actual data collected in a particular case? In other words, should courts focus on the *capacity* of the surveillance technology or the *actual* collection in the instant case? The Supreme Court has never offered this type of definitional deconstruction of technical/technological questions, but figuring out how to measure the unit of surveillance is key to properly analyzing the privacy and security risks of new technologies.

As will be discussed first in this Subpart, and then again applied to the Baltimore surveillance planes and the pole camera in *Tuggle* discussed in Part III, the nature of the framing choices will shape the ultimate constitutional conclusions. In fact, the definitional choices may be key to properly analyzing the Fourth Amendment risks of new surveillance technologies.

1. Tool or System

One critical question a court must ask about a surveillance technology is whether it should be considered a surveillance tool or a surveillance system. Early Fourth Amendment cases involved tools. The thermal imaging device in *Kyllo* was a handheld device to be used by an individual agent.[230] It was a standalone tool to measure heat levels from a particular house.[231] Similarly, the flyover cases in *California v. Ciraolo* and *Florida v. Riley* involved ordinary cameras taking photos of individual yards.[232] Even the "wiretap" in *Katz* was a

230. Brief for the United States, Kyllo v. United States, 553 U.S. 27 (2001) (No. 99-8508), 2000 WL 1890949, at *6 ("A thermal imager is able to detect infrared radiation. The imager gathers the infrared radiation that is emitted from the outside surface of the object at which it is pointed. The imager then converts what it has detected into a visible image that it displays on a screen. An imager is passive; it does not send out any rays. It is similar to a camera in that respect, except that a camera collects energy from the visible range of the electromagnetic spectrum, while imagers collect information from the infrared range. When the Agema 210 imager detects areas that are relatively warm, it displays them as white; when it detects areas that are relatively cool, it displays them as black; and when it detects areas between the extremes, it displays them as shades of gray. A polarity invert button on the imager changes the warmer spots from white to black and the cooler spots from black to white. The Agema 210 imager shows only relative heat patterns; it does not measure temperature in absolute terms." (citations omitted)).

231. *Id.* at *8 ("Detective Haas performed the thermal scan at issue in this case from the passenger seat of Agent Elliott's vehicle across the street from the front of petitioner's house. He then drove across the street and viewed the building from the back of the house. A videotape recording of the thermal scan of petitioner's house shows that the exterior of the center building (petitioner's house) is radiating more heat than the exterior of the other two buildings." (citations omitted)).

232. California v. Ciraolo, 476 U.S. 207, 209 (1986) ("Officer Shutz, who was assigned to investigate, secured a private plane and flew over respondent's house at an altitude of 1,000 feet, within navigable airspace; he was accompanied by Officer Rodriguez. Both officers were trained in marijuana identification. From the overflight, the officers readily identified marijuana plants 8 feet to 10 feet in height growing in a 15- by 25-

physical recording device affixed by hand to a single phone booth.[233] In contrast, the CSLI system in *Carpenter* was a vast network of cell towers that provided a nationwide system of data capture, and the *Jones* case involved a global satellite tracking system.[234]

The reason why the tool/system distinction matters is that along the continuum of data collection, the closer you get to a system of surveillance, the more the Fourth Amendment issues raised in *Riley*, *Jones*, and *Carpenter* become relevant.[235] Issues of aggregation, retrospective analysis, arbitrary use, overcollection, and thus privacy and security become greater with networked systems of surveillance.[236] While never stated as such, as discussed in Part II.A, the Supreme Court has mapped out a growing concern with mass surveillance systems (as opposed to mere surveillance tools).

The tool/system question raises the hard definitional issue of "what is the technology" being challenged. For courts, one question is whether their analysis should focus on an isolated data point (i.e., a sensor alert or video clip), or whether should courts visualize the technology as part of a larger digital surveillance network. As but one example, a standalone surveillance camera has been a staple of policing for many years. As a policing tool, the camera records the events occurring before it. The camera offers a limited view in terms of scale, scope, and duration and is regularly used as evidence. *Carpenter*, following a long line of other cases, carved out this type of conventional surveillance camera as not of Fourth Amendment concern.[237]

But harder questions emerge when this camera is considered part of a larger system of surveillance cameras. If, for example, the camera is linked to tens of thousands of other cameras (as in Chicago and New York City) such that a police investigator can track physical movement and activity day after day and block by block, does that change the analysis?[238] Or, would a linked camera system connected to license plate data or sensor data from e-bikes or e-scooters require different considerations?[239] Or, what if that linked system also included

---

foot plot in respondent's yard."); Florida v. Riley, 488 U.S. 445, 448 (1989) ("When an investigating officer discovered that he could not see the contents of the greenhouse from the road, he circled twice over respondent's property in a helicopter at the height of 400 feet. With his naked eye, he was able to see through the openings in the roof and one or more of the open sides of the greenhouse and to identify what he thought was marijuana growing in the structure.").

233. Brief for Petitioner, Katz v. United States, 389 U.S. 347 (1967) (No. 35), 1967 WL 113605, at *5 ("The recorder microphone was taped onto the booth and no part of the microphone physically penetrated the telephone booths.").

234. *See* Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018).

235. Ferguson, *supra* note 40, at 1140–41 (describing how courts can analyze systems of surveillance).

236. *Id.*

237. *Carpenter*, 138 S. Ct. at 2220 ("We do not . . . call into question conventional surveillance techniques and tools, such as security cameras.").

238. Higgins, *supra* note 136.

239. Brayne, *supra* note 120, at 300–01 ("In the largest Domain Awareness System, the NYPD partnered with Microsoft to collect information from closed-circuit surveillance cameras, ALPRs, radiation sensors, and other sensors to match with police databases."); Williams, *supra* note 32; JOHN S. HOLLYWOOD

uploaded personal data about an individual's prior convictions, prior police contacts, or social network connections?[240] In such a system, could a court appropriately address the privacy concerns by simply focusing on a single camera feed or isolated image, thereby ignoring the rest of the networked system?

Many persistent surveillance technologies tend to fall on the system side of the line and thus raise these hard Fourth Amendment questions. For courts evaluating whether the challenged technology is a tool or a system, the following questions should be asked. First, does the technology at issue, in fact, involve multiple technologies (different vendors, inputs, capabilities, data streams), suggesting a system rather than a single tool? Second, is the technology designed for standalone, particularized use (tools generally are, systems are not)? Third, is there a network effect such that the combination of tools creates a qualitatively different thing to analyze? Seeing the system of surveillance—including the backend capabilities after the data collection—changes the calculus.

For our purposes, questions about the unit of surveillance being measured offer a clarifying analytical framework. The answers force courts to see that their decision about what the technology *is* may also impact the Fourth Amendment analysis about whether the technology would invade a reasonable expectation of privacy. Artificially narrowing a focus to a particular tool may ignore the real privacy or security risks at issue from a larger interconnected surveillance system.

2. *Actuality or Capacity*

A second question courts must address is whether to focus on the actual data captured or the system's potential capacity to collect information. In other words, should judges evaluate the potential surveillance risks or just the actual digital evidence recovered in a particular case? In practice, for example, if the police promise to use a privacy-eviscerating technology in a way that is limited in practice (or by policy), are courts to evaluate the potential privacy harm or actual privacy harm of the technology?

ET AL., RAND CORP., USING VIDEO ANALYTICS AND SENSOR FUSION IN LAW ENFORCEMENT 4 (2018), https://www.rand.org/content/dam/rand/pubs/research_reports/RR2600/RR2619/RAND_RR2619.pdf ("The proliferation of internet-enabled digital video cameras and sensor devices (also known as the Internet of Things), combined with the ongoing fielding of conventional cameras, provides public safety agencies with huge technological opportunities.").

240. Certain cities like New York City have integrated police and prosecution databases that link this information together. *See* Ferguson, *supra* note 92, at 187–90 (describing the networks of surveillance in New York City); *see also* JENNIFER A. TALLON ET AL., CTR. FOR CT. INNOVATION, THE INTELLIGENCE-DRIVEN PROSECUTION MODEL: A CASE STUDY IN THE NEW YORK COUNTY DISTRICT ATTORNEY'S OFFICE 5 (2016), https://www.courtinnovation.org/sites/default/files/documents/IDPM_Research_Report_FINAL.PDF.

In traditional Fourth Amendment cases, this question was never asked. At issue in *Kyllo* was the actual thermal heat reading of Danny Kyllo's home.[241] In the overflight cases, the issue was the actual observation of the agents.[242] The Supreme Court did not ask what if the Drug Enforcement Administration agent had used the thermal imaging device on all the houses in the neighborhood or if the plane in *Ciraolo* had investigated everyone's home. The capacity of the technology as a form of potential mass surveillance was not directly addressed.[243]

In contrast, however, the focus in *Carpenter*, *Jones*, and *Riley* shifted to surveillance capacities. The frame of analysis greatly expanded from the myopic lens of older cases to the capacity of the surveillance to reshape privacy considerations. In *Carpenter*, for instance, the Court focused less on the actual data obtained (location data that corresponded with particular robberies of particular stores) and more on the potential capacity to track everyone with CSLI data (and without a warrant).[244] The Court's opinion largely ignored the privacy harm of the actual location data collected on Mr. Carpenter (he was in some stores), focusing instead on the privacy harm of collecting everybody else's data (data can show everyone in every store).[245] It was the capacity of the system to warrantlessly track everyone with a cellphone that guided the Court's analysis.[246]

The *Jones* concurrences also focused on the capacity of GPS tracking rather than the actual data about Antoine Jones. Of course, the tracking data was direct evidence to link Mr. Jones to the drug conspiracy, but the Fourth Amendment harms discussed in the concurrences went far beyond the few

241. *See* Kyllo v. United States, 533 U.S. 27, 29–30 (2001). The Agent used the thermal imaging device on a single night to examine a particular cluster of homes. *Id.* at 29. This was not a case of examining all the other homes in a neighborhood, although the technology certainly could have been used to gather that information.

242. *See* California v. Ciraolo, 476 U.S. 207, 212–13 (1986); Florida v. Riley, 488 U.S. 445, 462 (1989).

243. Justice Scalia did, however, acknowledge the concern with applying the Fourth Amendment to future technologies. In fact, the capacity factor of new technologies was indirectly raised in dicta. *Kyllo*, 533 U.S. at 35–36 ("We rejected such a mechanical interpretation of the Fourth Amendment in *Katz*, where the eavesdropping device picked up only sound waves that reached the exterior of the phone booth. Reversing that approach would leave the homeowner at the mercy of advancing technology—including imaging technology that could discern all human activity in the home. While the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development.").

244. Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018) ("The Government's position fails to contend with the seismic shifts in digital technology that made possible the tracking of not only Carpenter's location but also everyone else's, not for a short period but for years and years.").

245. *Id.*

246. Moreover, *Carpenter* interjects some real analytical fuzziness about when the search occurred. The Court uses the term *acquisition* to suggest that the warrantless police acquisition of location data from the cell phone company constituted the Fourth Amendment violation. *Id.* at 2220. Of course, what the police acquired at that moment was computer-generated locational data coordinates that had to be connected with other data to identify the owner of the cell phone. The Fourth Amendment harm was not the actual unrevealing information from that collection of binary code but the fact that a system existed with the capacity to identify individual cell phone owners at any location they visited.

geolocation clues that put Mr. Jones near the drug stash house.[247] Instead, the Justices focused on the capacity of GPS devices to track all individuals in indiscriminate and revealing ways.[248] The real fear of warrantless tracking involved the system's capacity to aggregate, link, infer, and reveal the privacies of life.[249] While the concurring Justices could have just focused on the actual location data collected and used in the prosecution, no Justice viewed the technology in such a narrow frame. While never stated as such, the concurring Justices focused on the capacity of warrantless GPS tracking to violate a reasonable expectation of privacy.[250]

Finally, in *Riley*, police only sought to use a few photographs from the camera function of the smartphone.[251] Yet, the Court's focus on the Fourth Amendment intrusion went far beyond the camera function. The Court analyzed the privacy harm by looking at the capacity of smartphones to reveal our personal data, including contacts, communications, calendar, finances, friends, associations, apps, and everything else on the device and the cloud.[252] The Court's analysis went far beyond the actual search of Mr. Riley's phone (for photos) and into the potential capacity of searching smartphones (for everything).

Courts addressing the question of whether persistent surveillance raises Fourth Amendment concerns, thus, must choose whether to look at the capacity of the surveillance system or the actual collection. As might be obvious, by choosing to focus on the capacity of a technology, courts will be more likely to see potential Fourth Amendment privacy harms.

One final complication arises from the capacity discussion and involves the ease of updating new technology. Because digital technology allows for upgrades, add-ons, integrations, and enhancements with relative ease, the capacity for a simple technology to expand is a real threat. For example, the 30,000 cameras in Chicago and the network of Project Green Light cameras in Detroit are capable of running facial recognition software on the camera

247. Justice Sotomayor cites *People v. Weaver* to suggest other privacy harms from long-term tracking. These harms were not alleged to be present in the *Jones* case but were harms when Justice Sotomayor thought of how GPS could be deployed against others. United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) ("Disclosed in [GPS] data . . . will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on[.]" (first alteration and omission in original) (quoting People v. Weaver, 909 N.E.2d 1195, 1199 (N.Y. 2009))).

248. *Jones*, 565 U.S. at 415. *See also id.* at 428 (Alito, J., concurring) (discussing other tracking technologies like toll cameras and sensors that can record movements—again, technologies that were not at issue in the case but that raise similar concerns about mass surveillance by the government).

249. *See Carpenter*, 138 S. Ct. at 2219.

250. *See Jones*, 565 U.S. at 427–31 (Alito, J., concurring).

251. Riley v. California, 573 U.S. 373, 379 (2014).

252. *Id.* at 395–96 (describing privacy-invading apps, Internet search results, and other digital clues that were not at issue in the prosecution of Mr. Riley).

systems.[253] While currently disabled (through an internal policy),[254] the capability to transform the network of observational surveillance into targeted investigative surveillance is one software update away from reality. Courts examining this capability question face hard choices. Because all technology can be updated, it cannot be the case that a futuristic capacity should change the constitutional analysis. But at the same time, legitimizing the constitutional use of technologies that can be upgraded in an instant seems equally limiting.

As has been discussed, these technology questions must be answered before the legal questions can be answered. In many cases, courts simply ignore these questions of what the "thing" is that needs to be analyzed. As will be discussed in the next Part, these predicate questions on the unit of surveillance are critical to the Fourth Amendment analysis.

III. PERSISTENT SURVEILLANCE AND THE FOURTH AMENDMENT APPLIED

For courts, untangling the threads of law, technology, and practice arising from persistent surveillance systems is a difficult task. The divided en banc court in *Leaders of a Beautiful Struggle* and the openly conflicted court in *Tuggle* reflect the challenges faced by judges trying to balance old doctrine and new technology. This Part seeks to apply the analytical and theoretical framework discussed above to show the strengths and weaknesses of the two opinions as well as to articulate a more coherent path forward.

As applied, courts should go through a three-step analysis to properly address the Fourth Amendment considerations of warrantless, persistent surveillance. First, courts should ask whether the "digital is different" Fourth Amendment argument convinces them to apply a new legal analysis freed from analog precedent. As discussed in Part I.C, the six "A" attributes likely make most long-term digital surveillance systems a different constitutional problem than traditional surveillance.

Second, courts need to determine the unit of surveillance they are evaluating. As discussed in the last Part, how you define "what the technology *is*" will shape the Fourth Amendment analysis. This step has been largely absent (or simply assumed away) in most cases addressing the Fourth Amendment harms of new surveillance.

Finally, as detailed in Part II, courts need to apply the constitutional clues provided by the Supreme Court about how to approach digital

253. *See* Ferguson, *supra* note 40; Harmon, *supra* note 32; *see also Project Green Light Detroit*, CITY OF DETROIT, https://detroitmi.gov/departments/police-department/project-green-light-detroit.

254. *See* Allie Gross, *Experts: Duggan's Denial of Facial Recognition Software Hinges on Three Words*, DETROIT FREE PRESS (July 16, 2019, 12:24 PM), https://www.freep.com/story/news/local/michigan/detroit/2019/07/16/duggan-war-of-words-surveillance-tech/1701604001/.

surveillance. Along a continuum, certain types of persistent surveillance technology will violate a reasonable expectation of privacy and thus the Fourth Amendment. This Part looks at the *Beautiful Struggle* and *Tuggle* cases to demonstrate how the three-step analysis should be applied consistent with these principles.

A. Step 1 – Persistent Surveillance Analysis

Is there a different persistent surveillance "act" occurring with the Baltimore surveillance planes? The answer is most certainly "yes." City-wide, all-day, digital capturing of everything with playback capabilities is about as different from a single fly-by of a particular house as can be imagined. Everyone in Baltimore was being surveilled every day.[255] The recordings were continuous (in twelve-hour bursts), *automated*, and vast in number.[256] The result is an *accumulation* of data that can be *accurately* accessed to search for particular clues or could be *aggregated* to find patterns of actions. Finally, the ability to quickly search for a particular location or activity and connect it with other investigative resources demonstrates the power of *accelerated* data flows and *actualized* digital searches. Almost everything about the Baltimore pilot was bigger in scale and scope, faster in finding objects, and more sweeping in its surveillance capabilities. All of the concerns of automation, accumulation, acceleration, accuracy, aggregation, and actualization are present in citywide aerial camera systems that record and link data for investigative purposes at scale.[257]

Long-term digital pole cameras require a closer examination to see if the act of surveillance is different from more conventional forms of police monitoring with video cameras. The surveillance act is *automated* with a continuous recording of a particular home. Similarly, while the *accumulation* of information is limited to a particular home, the depth of data collection is extensive. Everything and everyone coming and going outside the home is captured, analyzed, and studied for months. This accumulation of data is expansive and is also accessible because the digital nature of recording allows for retrospective searches, pattern matches, and identification. The ability to *accurately* quantify a person's patterns in and out of a home was certainly possible with live human observers in the past but would have been exceedingly difficult to maintain for eighteen months without getting caught. Plus, the *aggregation* allows inferences from accessing data about actions, trips, times, and associations, which is probably more revealing than other forms of monitoring. The digital nature of storage, retrieval, accessibility, search capabilities, and matching technologies does make these more sophisticated

255. Leaders of a Beautiful Struggle v. Balt. Police Dep't, 2 F.4th 330, 334 (4th Cir. 2021).

256. *Id.*

257. *See supra* Part I.C (setting out the six "A" attributes of persistent surveillance).

video collection systems different enough from traditional police video surveillance to warrant a different analytical approach. While the accumulation and aggregation capabilities are not as significant as the citywide aerial cameras, the automation, acceleration, accuracy, and actualization make this a different type of video surveillance than more conventional surveillance cameras.[258]

To say that the Baltimore surveillance planes or *Tuggle*'s pole camera are different from traditional surveillance does not make their warrantless use unconstitutional under the Fourth Amendment. But the different nature does flag the need for a new analytical approach to examine the constitutionality of persistent surveillance technologies.

B. Step 2 – The Systems Analysis

The second step in the analysis is what I call the "systems question." The systems question focuses on the unit of surveillance and asks if the particular technology fits within a network of other existing surveillance capabilities. For example, the fact that footage from the Baltimore aerial planes could be cross referenced to ground level cameras, automated license plate readers, gunshot detectors, and other technologies changes the unit of surveillance.[259] Whereas before, when a court might just focus on the aerial images, the systems question broadens the analysis to examine the entire network of surveillance being deployed. As discussed, this requires courts to make two further definitional choices when analyzing any technology for Fourth Amendment purposes.[260] First, courts must decide whether they are analyzing a stand-alone surveillance tool or a surveillance system; second, courts must decide whether they should be analyzing the current capabilities or future capabilities of this technology.

This systems question has remained unexamined in court decisions around surveillance technology. And, to be fair, there are good reasons why. First, courts were (and are) limited to the cases and controversies before them and are not supposed to speculate about future or possible harms.[261] Second, for many early cases, police surveillance was considered a tool because it was, in fact, a tool (and did not involve sophisticated or connected systems).[262] Third, police searches were considered active, not passive endeavors.[263] Police affirmatively would go out to find particular information rather than setting up

258. *Id.*

259. *See supra* Part II.B.

260. *See supra* Part II.B.

261. City of Los Angeles v. Lyons, 461 U.S. 95, 101 (1983) ("It goes without saying that those who seek to invoke the jurisdiction of the federal courts must satisfy the threshold requirement imposed by Art. III of the Constitution by alleging an actual case or controversy.").

262. *See supra* notes 230–233 (discussing the surveillance tools at issue in earlier cases).

263. *See* Ric Simmons, Terry *in the Age of Automated Police Officers*, 50 SETON HALL L. REV. 909, 934 (2020) (discussing the consequences of automated, passive surveillance technologies).

automated monitoring systems to collect generalized information and only later go back to find something specific.[264] Courts chose to evaluate the active act of investigation and not to evaluate the passive systems of data collection or retrieval. Finally, the nature of the surveillance technologies is not always well understood. Most police investigatory systems lack transparency for a host of tactical and cultural reasons, so seeing the scope and interconnections of the systems is not always easy.

Yet, while understandable, the failure to frame the arguments around the systems question has led courts to undervalue the dangers of new surveillance. Again, the *Beautiful Struggle* and *Tuggle* cases offer helpful examples to see how the definitional question of what the technology *is* can explain the Fourth Amendment analysis and outcome. The next Subparts show how the en banc Fourth Circuit got the framework mostly correct in its analysis of the Baltimore surveillance planes and how the Seventh Circuit in *Tuggle* failed to address the systems question.

1. Persistent Surveillance Systems

In *Leaders of a Beautiful Struggle*, three courts—a district court, the United States Court of Appeals for the Fourth Circuit, and the en banc Fourth Circuit—all addressed the unit of surveillance question in different ways leading to different results.[265] While none of the courts explicitly recognized the systems question issue, the definition of the technology at issue shaped how each court saw the Fourth Amendment problem to be decided.

a. System or Tool

Was the Baltimore PSS/AIR program a surveillance system or tool? It is pretty easy to make an argument that the Baltimore Persistent Surveillance System is a "system of surveillance" because the admission exists right there in the name.[266] By design, the aerial cameras were meant to work with other surveillance devices to create a network of monitoring capabilities.[267] The aerial planes were designed to link up to other city cameras and ALPRs to identify a

264. *Id.*

265. Leaders of a Beautiful Struggle v. Balt. Police Dep't, 456 F. Supp. 3d 699 (D. Md.), *aff'd*, 979 F.3d 219 (4th Cir. 2020), *rev'd en banc*, 2 F.4th 330 (4th Cir. 2021).

266. In addition, the Baltimore program was named the Aerial Investigation Research (AIR) program—with the investigation nomenclature also suggesting that this was an investitive surveillance system.

267. ANDREW R. MORRAL ET AL., RAND CORP., EVALUATING BALTIMORE'S AERIAL INVESTIGATION PILOT PROGRAM: INTERIM REPORT 9 (2021) ("When people or vehicles were seen to pass CitiWatch cameras or license plate reader systems, AIR analysts would call up those systems and download video or license plate information that could help to identify cars, drivers, passengers, or pedestrians of interest.").

suspect and/or vehicle.[268] The networked nature of the surveillance was evident in the interconnectedness of investigative resources[269] and in the resulting investigative product, which included analyst work-product all uploaded to a cloud-based service hosted on Evidence.com.[270]

As recognized by the en banc Fourth Circuit, the aerial images did not stay in the planes but were sent to analysts for processing and storage at "ground stations."[271] The data was connected to ground level police systems through software that integrated other sensor information from existing police databases.[272] The data was stored and searchable for at least forty-five days, sometimes more.[273] Analysts would summarize the data in written investigative reports for police use.[274]

This analytical move—to define the Baltimore AIR planes as a system of surveillance and not merely a camera-based tool[275]—led the en banc *Beautiful*

268. BARRY FRIEDMAN ET AL., POLICING PROJECT AT N.Y. UNIV. SCH. OF L., CIVIL RIGHTS AND CIVIL LIBERTIES AUDIT OF BALTIMORE'S AERIAL INVESTIGATION RESEARCH (AIR) PROGRAM 14 (2020) ("The most useful of these ground technologies is BPD's high-definition cameras, known as 'CitiWatch cameras.' Each of these cameras has a field of view spanning nearly two city blocks. The video resolution of these cameras is high enough to, on occasion, show a vehicle's license plate number, make, and model, or the face, clothing, or other identifying characteristics of an individual in the vehicle. PSS has direct access to CitiWatch footage—in one sample investigation we reviewed, one tracked subject passed by over 70 cameras as they moved through Baltimore—though they do not have the ability to pan or zoom in. PSS analysts select and share still images from these cameras with detectives.").

269. *Id.* at 8 ("Because the resolution is relatively low, the use of information from ground-based surveillance technologies—such as red-light cameras, automated license plate readers (ALPRs), and CitiWatch cameras—both assist in tracking and are critical to helping analysts find identifying information about a specific car or individual. This is why the aerial, ground-based, and human resources should be thought of as one composite system.").

270. MORRAL ET AL., *supra* note 267, at 10–11 ("[T]he final product from the AIR analysis was to be an evidence package—a briefing that would include aerial imagery, tracks, and annotations about suspects' behaviors and activities; video collected from CitiWatch cameras; images of buildings or locations drawn from Google Street View; and other information the AIR analysts could assemble on the people, vehicles, and locations related to the investigations. These evidence packages would be uploaded to the BPD's electronic evidence management system, Evidence.com, where they would be available to detectives, their supervisors, and prosecutors and defense attorneys.").

271. Leaders of a Beautiful Struggle v. Balt. Police Dep't, 2 F.4th 330, 334 (4th Cir. 2021) ("The planes transmit their photographs to PSS 'ground stations' where contractors use the data to 'track individuals and vehicles from a crime scene and extract information to assist BPD in the investigation of Target Crimes.'").

272. *Id.* ("PSS may 'integrate . . . BPD systems' into its proprietary software 'to help make all of the systems work together to enhance their ability to help solve and deter crimes.' The PSA lists BPD's dispatch system, 'CitiWatch' security cameras, 'Shot Spotter' gunshot detection, and license plate readers as systems to be integrated. As a result, AIR reports may include ground-based images of the surveilled targets from 'the cameras they pass on the way.'" (omission in original) (citation omitted)).

273. *Id.* ("AIR data is stored on PSS's servers, and '[PSS] will retain the AIR imagery data for forty-five days.' PSS maintains the reports, and related images, indefinitely as necessary for legal proceedings and until relevant statutes of limitations expire." (alteration in original) (citations omitted)).

274. *Id.* ("PSS aims to provide an initial briefing within 18 hours and a more in-depth 'Investigation Briefing Report' within 72 hours. The reports may include, from both before and after the crime: 'observations of driving patterns and driving behaviors'; the 'tracks' of vehicles and people present at the scene; the locations those vehicles and people visited; and, eventually, the tracks of the people whom those people met with and the locations they came from and went to.").

275. *Id.* at 345 ("Regarding AIR data as just 'one more investigative tool' does exactly what the Supreme Court has admonished against; it allows inference to insulate a search.").

Struggle court to hold that accessing this collected information was a violation of an expectation of privacy.[276] It was accessing this system of collected investigatory data that created the Fourth Amendment violation:

> The AIR program records the movements of a city. With analysis, it can reveal where individuals come and go over an extended period. Because the AIR program enables police to deduce from the whole of individuals' movements, we hold that accessing its data is a search, and its warrantless operation violates the Fourth Amendment.[277]

In so shifting the debate to systems from tools, the en banc *Beautiful Struggle* court also shifted the focus away from the self-imposed technological limits of the AIR cameras.[278] Unlike the district court, which focused on the limited details revealed by the images, the en banc Fourth Circuit focused on the interconnected nature of the networks.[279] In other words, law enforcement's access to the PSS dataset of all Baltimore residents—movements, vehicles, homes, associations, etc.—violated a reasonable expectation of privacy.[280] Readers can judge for themselves about whether they are convinced by the constitutional argument, but the en banc court's answer to the systems question clearly shaped the outcome.

b. Actuality or Capacity

As discussed in Part II, the actuality/capacity debate is also an important question to be resolved. Are judges evaluating the potential privacy risk from growing surveillance technologies or the actual collection in a particular case? This interpretive question is made even more difficult in a case like Baltimore where the ambitions of the planned police surveillance were thwarted by bureaucratic roadblocks, making the actual practice less invasive of privacy than

276. *Id.* ("[B]ecause AIR data is what enables deductions from the whole of individuals' movements, the Fourth Amendment bars BPD from warrantless access to engage in that labor-intensive process.").

277. *Id.* at 346.

278. FRIEDMAN ET AL., *supra* note 268, at 12 ("Although PSS cameras are powerful enough to deliver high resolution images, . . . for technological reasons, there is a tradeoff between coverage and definition of objects at ground-level. PSS prioritizes a wide coverage area over high definition. PSS also believes it can address privacy concerns preemptively by programming a resolution limit into its software, thereby making it impossible to identify anyone from the air. This resolution limitation is built into the photograph—zooming cannot improve the resolution.").

279. *See Leaders of a Beautiful Struggle*, 2 F.4th at 341–46.

280. *Id.* at 344 ("But to identify a 'search,' we identify an invasion of a reasonable privacy expectation. To do that, we consider not only the raw data, but what that data can reveal. BPD can deduce an individual's identity from AIR data, other available information, and some deductive reasoning. The integration of police information systems supports that conclusion. When coupled with a highly precise map of movements across at least 45 days, these abilities enable police to glean insights from the whole of individuals' movements. Therefore, when BPD 'accesses' AIR data, it invades the recorded individuals' reasonable expectation of privacy, conducting a search." (citation omitted)).

if it had worked as designed.[281] At the same time, on occasion, the police practices exceeded the self-imposed policy limits.[282] The question becomes should courts evaluate the stated *policy*, the *practice*, or the *potential* of the surveillance system when evaluating Fourth Amendment questions?

For example, the en banc *Beautiful Struggle* court criticized the narrowness by which the trial court evaluated the AIR program's self-imposed limits. The en banc court stated:

> The district court's conclusion arose from its read of the facts: "the AIR pilot program has limited location-tracking abilities" because it "will only depict individuals as miniscule dots moving about a city landscape"; the planes "will not fly at night and cannot capture images in inclement weather"; and "gaps in the data will prohibit the tracking of individuals over the course of multiple days." From that premise, it believed the AIR program could not expose the "privacies of life." The district court misapprehended the AIR program's capabilities.[283]

As discussed, the en banc court expanded its analysis from the stated policies to cover the potential use of the data once captured and stored. By governmentally-approved plan, the Baltimore AIR project envisioned a networked system of interconnected databases, cameras, and sensors, which is what the court evaluated.[284]

Ironically, the actual practice in Baltimore followed neither the limited policy nor the possible potential uses. Due to a series of delays and bureaucratic roadblocks, the Baltimore Police Department failed to create the surveillance system it envisioned during the pilot project.[285] For example, certain investigative systems (ShotSpotter and ALPR) were never connected to the system (as planned) due to legal concerns and some bureaucratic turf battles.[286] Interestingly, both the en banc court and the trial court ignored this reality and decided the case on the written policies and promises of how the AIR program was supposed to work.[287]

---

281. It is unclear whether the information-sharing roadblocks were intentional or unintentional. The political support for the Baltimore AIR program changed over time creating some ambiguity about why the information-sharing barriers were created.

282. Brief of the Policing Project as Amicus Curiae in Support of Neither Party and in Support of Rehearing or Rehearing En Banc at 7–8, Leaders of a Beautiful Struggle v. Balt. Police Dep't, 831 F. App'x 662 (4th Cir. 2020) (No. 20-1495), 2020 WL 7024182, at *7–8 (describing how certain police investigations exceeded the scope of the established policies).

283. *Leaders of a Beautiful Struggle*, 2 F.4th at 340 (citations omitted).

284. *See id.* at 341–46.

285. *See* MORRAL ET AL., *supra* note 267, at 15 ("Although PSS had hoped to access the BPD's [computer-aided dispatch (CAD)] system so that it could begin investigating [memorandum of understanding (MOU)] crimes the moment they were called in, the BPD did not provide that access.").

286. *See id.* ("Similarly, PSS had hoped to have direct access to the BPD's ShotSpotter and license plate reader systems; the MOU between the city and PSS allowed for that access. However, the BPD did not ultimately authorize PSS's direct access to either of these systems.").

287. This reality leaves open a fascinating (and unanswered) question: Could a program like Baltimore's surveillance planes survive Fourth Amendment scrutiny because their planned unconstitutional

c. Conclusion on Persistent Surveillance Systems

One can debate whether *Leaders for a Beautiful Struggle* was correctly decided under Fourth Amendment precedent, but the impact of the unit of surveillance framing is pretty clear. Because the en banc court focused its attention on the systems of surveillance and because it recognized the potential risks arising from growing surveillance capabilities, the court found a violation of a reasonable expectation of privacy from these planes and related data systems. A narrow framing—like that of the trial court—would likely have resulted in a different outcome.

2. Long-Term Police Cameras

Tuggle presents another fascinating case study of how courts choose to define and delimit the technology. For example, the *Tuggle* court chose to define the pole camera as a tool focusing on the frontend images captured and ignoring the back-end data collection, analysis, and storage.[288] In addition, the *Tuggle* court focused on the actual collection, ignoring the potential of how that private information could be connected to larger investigatory systems for additional uses.[289]

I take the position here that these choices were in error, and a proper understanding of the unit of surveillance shows that the *Tuggle* court artificially narrowed the question of the technology at issue—a choice that resulted in an equally cabined (and erroneous) Fourth Amendment holding.

a. Tool or System

Throughout the opinion, the *Tuggle* court considered the pole cameras as stand-alone tools.[290] The three cameras were described as merely technological enhancements of police officers' eyesight, focusing on what limited things could

surveillance happened to be less powerful due to various bureaucratic or technological roadblocks? Could simple incompetence save Orwellian surveillance plans from Fourth Amendment challenge? *See* Leaders of a Beautiful Struggle v. Balt. Police Dep't, 456 F. Supp. 3d 699 (D. Md.), *aff'd*, 979 F.3d 219 (4th Cir. 2020), *rev'd en banc*, 2 F.4th 330 (4th Cir. 2021).

288. United States v. Tuggle, 4 F.4th 505, 511 (7th Cir. 2021) ("The focus of this appeal is the government's warrantless use of three video cameras affixed to nearby utility poles to monitor Tuggle's residence.").

289. *Id.* at 516 (describing the role of cameras in society as an argument for why this pole camera did not violate an expectation of privacy but ignoring any of the connected and collected streams of information linked to those cameras).

290. The word "tools" is even used to describe security cameras that did not offend the Fourth Amendment. *See id.* at 526 (analogizing pole cameras to security cameras and citing to the Supreme Court in *Carpenter* which stated it "was *not* 'call[ing] into question conventional surveillance techniques and tools, *such as security cameras*.'" (alteration in original) (quoting Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018))).

be seen by the cameras.[291] A more complete analysis, however, would view the video monitoring as part of a larger system of surveillance.

As an initial matter, it is simply not accurate only to consider the video footage and not the vast stores of digital information that were part of this investigation. They are two parts of a whole. The cameras provided live video feeds but also generated stored data that went back to FBI headquarters to be analyzed.[292] Investigating officers had database access to a year and a half of lived experience—all collected, searchable, and usable to identify people, things, patterns, and events.[293] A proper analysis of what was happening to *Tuggle* was that a digital dossier was being created and continuously maintained to further a criminal investigation. Further, that digital dossier could be connected to other investigative resources in the network. The data in the dataset—license plates, photographs, and other identifying clues—were valuable because they could be connected to other information sources.

The point is not that the Fourth Amendment should have to encompass all of these connected investigatory acts as part of the search inquiry (although perhaps it should), but that the court's choice to see digital pole cameras as mere tools and not connected to a network of police information systems is misleading. There is a world of difference between police using a camera to watch your front door and a police officer being able to access a saved, searchable database of images from your front door for the past eighteen months connected to other police datasets of personal information. The camera, the creation of a dossier, and the search capabilities of that video data base are all connected in a system of surveillance and thus must be analyzed as one.

b. Actuality or Capacity

Thinking about pole-camera surveillance as a connected system also raises the "actuality or capacity" question. *Tuggle* is a strange case because while the court narrowed its analysis to the actual images captured around the home, it foresaw the potential danger of this type of digital surveillance.[294] The opinion opens by giving voice to Judge Flaum's internal struggle about the potential capacity of big data policing:

---

291. *Id.* at 514–15 (citing approvingly to *United States v. Knotts*, 460 U.S. 276, 282 (1983), to argue that cameras as mere enhancements did not violate a reasonable expectation of privacy).

292. *Id.* at 511 ("While officers frequently monitored the live feed during business hours, they could later review all the footage, which the government stored at the Federal Bureau of Investigation office in Springfield, Illinois.").

293. *Id.* at 511–12 ("The cameras provided substantial video evidence that supported the government's eventual indictment of Tuggle (and others). The officers tallied over 100 instances of what they suspected were deliveries of methamphetamine to Tuggle's residence. Camera footage depicted individuals arriving at Tuggle's home, carrying various items inside, and leaving only with smaller versions of those items or sometimes nothing at all.").

294. *Id.* at 509–10.

> One day, in a not-so-distant future, millions of Americans may well wake up in a smart-home-dotted nation. As they walk out their front doors, cameras installed on nearby doorbells, vehicles, and municipal traffic lights will sense and record their movements, documenting their departure times, catching glimpses of their phone screens, and taking note of the people that accompany them.
>
> These future Americans will traverse their communities under the perpetual gaze of cameras. Camera-studded streets, highways, and transit networks will generate precise information about each vehicle and its passengers, for example, recording peoples' everyday routes and deviations therefrom. Upon arrival at their workplaces, schools, and appointments, cameras on buildings will observe their attire and belongings while body cameras donned on the vests of police and security officers will record snippets of face-to-face or phone conversations. That same network of cameras will continue to capture Americans from many angles as they run errands and rendezvous to various social gatherings. By the end of the day, millions of unblinking eyes will have discerned Americans' occupations and daily routines, the people and groups with whom they associate, the businesses they frequent, their recreational activities, and much more.
>
> The setting described above is not yet a total reality. Nonetheless, we are steadily approaching a future with a constellation of ubiquitous public and private cameras accessible to the government that catalog the movements and activities of all Americans. Foreseeable expansion in technological capabilities and the pervasive use of ever-watching surveillance will reduce Americans' anonymity, transforming what once seemed like science fiction into fact.[295]

One might assume that after this striking articulation of dystopian surveillance the *Tuggle* court might suggest a constitutional response to limit persistent surveillance with pole cameras. And yet, the *Tuggle* court found no Fourth Amendment search by narrowing the question to the actual collection of images in the case.[296]

To be clear, it obviously would be inappropriate for a federal court to decide the constitutionality of a particular police action on a potential parade of horribles that could (someday) arise from Orwellian technological surveillance.[297] But even within a more limited framework, the *Tuggle* court ignored the capacity issues that might arise from the technology before it. More precisely, the investigating agents in *Tuggle* essentially created Judge Flaum's "smart-home" -like hypothetical with cameras watching the door and vehicles and "documenting their departure times" with a corresponding reduction of

295. *Id.* at 509.

296. *Id.* at 529.

297. Margaret Hu, *Orwell's* 1984 *and a Fourth Amendment Cybersurveillance Nonintrusion Test*, 92 WASH. L. REV. 1819, 1862–63 (2017) ("References to George Orwell's *1984* conjure up specific and widely recognized images of a police state, mass surveillance, torture, tyranny, and thought crime. *1984* often serves as a placeholder to explain how the law has failed to preserve individual autonomy, dignity, and rights in the face of changing social and political circumstances." (footnotes omitted)).

anonymity and privacy.[298] What the *Tuggle* court imagined as a future technology threat was actually occurring in the present, with real impacts on familial privacy and associational liberty.

In addition, the capacity argument should also reflect what might happen in the future. Under *Tuggle*'s logic, police can place surveillance cameras outside any home, for any reason, for years, and store all of the searchable information forever. The homes of federal judges, journalists, activists, lawyers, abortion doctors, abolitionists, NRA members, imams, rabbis, priests, and politicians can be watched and digital dossiers created all without judicial authorization or any constitutional limit. In addition, under *Tuggle*'s reasoning, the collected dataset can be integrated with other information (such as license plate readers, facial recognition, court data, and financial information) and the video dossier of a life and family can be used to connect the dots about a life for investigation purposes. Without a constitutional check, the ability to create this surveillance panopticon is only limited by the availability of cameras and the willingness of police to use them on whomever they choose. While the actual data of footage around Tuggle's house ranged from mundane to embarrassing to incriminating,[299] the capacity to collect was limitless.

c. Conclusion on the Pole Cameras

Pole camera cases have been litigated for years now with conflicting results.[300] While one can sympathize with Judge Flaum's struggle with the law in *Tuggle*, I argue that the choice to narrowly define the unit of surveillance is what creates the finding of no Fourth Amendment violation. Choosing to see the pole cameras as a tool and limiting the focus to the actual camera images misses the real systemic privacy harms. If seen as a system of stored surveillance footage, the Fourth Amendment analysis changes.

***

This Subpart has sought to demonstrate that the courts' choice of the unit of surveillance may be more significant than other factors in shaping an outcome. How a court sees the technology at issue and defines the scope of

298. *Tuggle*, 4 F.4th at 509.

299. Appellant's Brief and Appendix at 21–22, United States v. Tuggle, 4 F.4th 505 (7th Cir. 2021) (No. 20-2352), 2021 WL 320116, at *21–22 ("Although the pole cameras were stationary, the cameras monitored everything in the vicinity of Mr. Tuggle's residence. The Government was able to use the cameras to determine Mr. Tuggle's habits, such as when he left and returned to his residence. The pole cameras were also deployed to observe and record Mr. Tuggle walking outside in his boxers and urinating in his front yard, amongst other private activities.").

300. *Compare* United States v. Trice, 966 F.3d 506, 516–20 (6th Cir. 2020), *and* United States v. May-Shaw, 955 F.3d 563, 567–69 (6th Cir. 2020), *and* United States v. Cantu, 684 F. App'x 703, 704–06 (10th Cir. 2017), *with* Commonwealth v. Mora, 150 N.E.3d 297, 313 (Mass. 2020), *and* People v. Tafoya, 494 P.3d 613, 616 n.4 (Colo. 2021), *and* United States v. Houston, 965 F. Supp. 2d 855, 898 (E.D. Tenn. 2013).

surveillance will likely guide Fourth Amendment analysis. And as more persistent surveillance technologies emerge, the more necessary the analysis will become.

C. Step 3 – Constitutional Analysis

As developed in Part II, the Fourth Amendment is in flux when it comes to responding to the threat of powerful new surveillance technologies. But despite the uncertainty, a framework does exist for determining whether technologies—properly defined by the correct unit of surveillance—violate an expectation of privacy and are thus unreasonable searches without a warrant. The analysis detailed below asks which side of the line a particular persistent surveillance technology falls on with the understanding that a Fourth Amendment violation exists when enough of these factors are found. Again, the framework asks the following questions:[301]

- Digital or Analog Technology?
- Aggregated or Single-Use Information?
- Retrospective or Ephemeral Capabilities?
- Superpower or Enhancement?
- Impacting Associational Freedoms or Not?
- Arbitrary or Targeted Collection?
- Permeating or Cabined Surveillance?

A surveillance technology that falls consistently on the side of the first choice in each option is more likely to offend sensibilities around what society considers a reasonable expectation of privacy.

1. Baltimore's Persistent Surveillance Systems as a Search

The aerial planes and connected ground-level technologies that make up the Baltimore Persistent Surveillance System hit all of the elements of what would be more likely considered a search along a continuum of clues provided by the Supreme Court. The technologies are digital, with aggregating and retrospective capabilities.[302] Accessing the stored digital footage allows time-machine-like powers[303] (far greater than the GPS data in *Jones* or the CSLI in

301. This framework is set out in Part II.

302. Leaders of a Beautiful Struggle v. Balt. Police Dep't, 2 F.4th 330, 342 (4th Cir. 2021) ("[T]he program enables photographic, retrospective location tracking in multi-hour blocks, often over consecutive days, with a month and a half of daytimes for analysts to work with. That is enough to yield 'a wealth of detail,' greater than the sum of the individual trips.").

303. *Id.* at 341 ("Because the data is retained for 45 days—at least—it is a 'detailed, encyclopedic,' record of where everyone came and went within the city during daylight hours over the prior month-and-a-half. Law enforcement can 'travel back in time' to observe a target's movements, forwards and backwards." (citation omitted)); *see also* MORRAL ET AL., *supra* note 267, at 8 ("Frame rates from the cameras would be

Carpenter). Police can literally follow a suspect's path back in time from a criminal event or for several days. The aerial tracking itself is quite revealing, identifying types of vehicles, home addresses, types of buildings, friends, associates, paths, and patterns.[304] More importantly, when the location data is connected with other police investigative technologies like street-level cameras, automated license plate readers, and mapping technologies, a more complete picture of movements and inferences therefrom can be developed.[305] A vehicle image captured by the aerial camera could be linked to a street level camera to identify the license plate, driver, or address where it was parked.[306] Thus, the same locational tracking concerns that revealed the privacies of life in *Jones* and *Carpenter* are present but for an even greater number of people and a longer time period.[307] For forty-five-plus days any public trip, activity, or pattern could

sufficiently high to provide a nearly continuous video of events below, allowing PSS analysts to track suspects and witnesses both forward and backward in time from any crime scenes captured by the aircraft.").

304. MORRAL ET AL., *supra* note 267, at ix ("Using aerial imagery, analysts would construct annotated tracks displaying the paths traveled by people and vehicles through the city before and after a crime, noting when suspects or witnesses appeared to spend time with cars, other vehicles, or in homes or buildings. When people or vehicles were seen to pass CitiWatch cameras or license plate reader systems, AIR analysts would use those systems to download video or license plate information that could help to identify cars, drivers, passengers, or pedestrians of interest.").

305. FRIEDMAN ET AL., *supra* note 268, at 14 ("PSS analysts can gain additional information by laying a track they have created atop a basic street level map using Google Earth. In this way, analysts can follow the track of a person or vehicle of interest to a particular address and inform BPD about the significance of those locations. For example, one PSS report determined that the target visited a shopping mall, a food market, and finally a gas station. In another investigation, an analyst noted that the target '[drove] to [a local] University,' and flagged that 'there are no classes going on currently.' In certain circumstances, particularly with large buildings or complexes, PSS even may be able to note if a subject entered a particular door, walked through a courtyard, or parked in a particular parking spot. Such tracking can help with identification of the vehicle or person. Still, the value of aerial maps, standing alone, is somewhat limited." (alterations in original)). For full disclosure, I was an unpaid Senior Technology Fellow at the NYU Policing Project from 2018–2021. I did not work on the Baltimore AIR Report and had no access to or influence on the analysis or drafting of the report.

306. *Id.* at 12 ("[A]t the level of resolution PSS is using, vehicles are represented by approximately 15–20 pixels. This means that PSS analysts sometimes can determine a vehicle's general color, general body-type, the direction the vehicle is facing, and other distinguishing characteristics, such as a sunroof. Analysts often can distinguish law enforcement and other emergency response vehicles from the aerial imagery alone, either from their appearance or from the vehicle's behavior. Furthermore, based on the direction a vehicle is facing, analysts often can determine if a person enters or exits a driver or passenger side door."); *see also id.* at 14 ("Another ground technology that is quite useful to PSS analysts is information provided by automatic license plate readers, or ALPRs. ALPRs take pictures of vehicle license plates, geo-stamping them with time and location. Although PSS analysts do not have direct access to ALPRs, they use ALPRs in two ways: First, by collaborating with BPD detectives, analysts can track an unknown car to an ALPR and then the detective can use the ALPR to obtain the license plate number. Second, BPD detectives can search the ALPR database for a specific vehicle of interest, and use the geo-stamp to alert PSS analysts, who then can begin tracking that vehicle backward and forward in time from the ALPR.").

307. *Leaders of a Beautiful Struggle*, 2 F.4th at 343 ("That Defendants chose to limit data collection to daylight hours and a certain resolution does not make the AIR program equivalent to traditional, short-term surveillance. AIR data is a photographic record of movements, surpassing the precision even of GPS data and CSLI, which record variable location points from which movements can be reconstructed. And while the coverage is not 24/7, most people do most of their moving during the daytime, not overnight. Likewise, many people start and end most days at home, following a relatively habitual pattern in between. These habits,

be queried, analyzed, and used as evidence. This is a far greater privacy and liberty invasion that any of the single-use search cases blessed by the Supreme Court in prior eras.

The other identified factors also support a finding of a search. With the ability to watch an entire city from the sky, the aerial cameras provide police a superpower that is many magnitudes greater than any human capability even with enhancements.[308] A camera might be an enhancement, but a camera system that captures everything in public is something more. The Baltimore aerial cameras had the ability to take a photo every second and stich those photos together to create a map of human activity well beyond human capabilities.[309]

Individuals who valued political, religious, and personal freedom from monitoring risked being captured in the images—thus chilling associational freedoms. Activists, like those who brought the federal lawsuit, feared the collection of personal and political information about their activities.[310] And, even if not directed at activists specifically, the collection was overbroad, arbitrary, and permeating in nature.[311] Just the idea of an eye in the sky watching where you walk or travel chills protected First Amendment activities, mutes political expression, and raises concerns about the infringement of religious and personal liberty.[312]

While it is true that the cameras were not continuously running (the planes were set to fly for twelve hours, not twenty-four hours), some continuous

---

analyzed with other available information, will often be enough for law enforcement to deduce the people behind the pixels.").

308. *Id.* at 345 ("For all these reasons, the AIR program's surveillance is not 'short-term' and *transcends mere augmentation of ordinary police capabilities*. People understand that they may be filmed by security cameras on city streets, or a police officer could stake out their house and tail them for a time." (emphasis added)).

309. FRIEDMAN ET AL., *supra* note 268, at 8 ("PSS's planes are equipped with powerful cameras that take photographs capturing much of the city. The planes take one photo every second, which PSS's software stiches together to create a second-by-second 'map' of the activity below. Because the cameras are set to capture a wide area, images, once zoomed in, have low definition: cars appear as several pixels, and individuals as one to a few pixels. Although with this limited definition analysts can sometimes determine general information about a vehicle, such as its color, they cannot see something as specific as a license plate number, and they cannot identify individuals from the air.").

310. *Leaders of a Beautiful Struggle*, 2 F.4th at 335 ("Plaintiffs are grassroots community advocates in Baltimore. Their advocacy necessarily involves traveling through and being present outdoors in areas with high rates of violent crime. For example, Erricka Bridgeford leads Ceasefire Baltimore and, in that capacity, visits scenes of gun violence as soon as possible after a crime takes place.").

311. FRIEDMAN ET AL., *supra* note 268, at 14 ("AIR's aerial and ground-based components are mutually reinforcing. That is, the utility of aerial images is enhanced considerably with ground-level surveillance tools. Likewise, the aerial images allow BPD to maximize the value of existing ground-level surveillance technologies. Integrating these technologies makes it possible for BPD and PSS to identify the actual people being tracked, and to track their movements over time.").

312. United States v. Jones, 565 U.S. 400, 416 (2012) ("Awareness that the government may be watching chills associational and expressive freedoms. And the government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse.").

tracking over several days did occur.[313] Equally importantly, the permeating and long-term nature of the collection allowed investigators to go back to particular locations and connect the digital dots.[314] This could involve repeated searches of particular places and reliance on other investigative databases to link people, cars, and groups together.[315] In sum, all of the triggers that the Supreme Court has suggested might violate a reasonable expectation of privacy—namely, a digital, aggregating, retrospective superpower that arbitrarily chills associational freedom and permeates a society—applies to the Baltimore Persistent Surveillance System planes.

2. Long-Term Pole Cameras as a Search

Long-term pole cameras, like those utilized in *Tuggle*, again present a more complicated analysis. On the search side of the line, the cameras are digitally aggregating personal information and allow for retrospective searches by going back in time with the footage around the home. This long-term monitoring mirrors some of the aggregation concerns in *Jones* and *Carpenter*—i.e., that intensive surveillance reveals many of the privacies of life.[316]

In *Tuggle*, however, the Seventh Circuit asserted that aggregation was less revealing than *Jones* or *Carpenter* because the cameras did not connect the dots about *public* pieces of information about Tuggle's life.[317] The court emphasized:

> Unlike those technologies [GPS/CSLI], the cameras here exposed no details about where Tuggle traveled, what businesses he frequented, with whom he interacted in public, or whose homes he visited, among many other intimate details of his life. If anything, far from capturing the "whole of his physical

313. FRIEDMAN ET AL., *supra* note 268, at 11 ("In one case in particular, AIR was used to track a vehicle over 3 days and document 11 locations where the vehicle stopped.").

314. *Id.* at 15 ("[E]asier identification makes it possible for PSS to track persons and vehicles over multiple days. Although PSS's planes do not fly overnight, analysts can use ground surveillance to reidentify a person or vehicle on multiple days. For example, if PSS is tracking a vehicle on Day 1, they then can use ALPRs to find the vehicle again on Day 2 and continue tracking. That said, the ability to carry out a multi-day track can vary from case-to-case. If a car parks outside a home in the evening and does not move until the next morning, the reidentification and continuation of the tracking is relatively simple. Reidentification is also straightforward when a vehicle passes a nearby ALPR or CitiWatch camera. But in other cases, the reidentification process can require a fair amount of analyst work and is not guaranteed to succeed.").

315. *Id.* ("This integration of aerial and ground-surveillance can be used in a number of ways. First, it makes it far easier to identify an individual in a track that PSS is following. For example, once the aerial map identifies a subject crossing a ground device, PSS analysts can use the ground device to get a clear image of a license plate, which then can be cross referenced with DMV records. They also can obtain images of a person's face, which can then be shown to a witness or run through facial recognition software. In one investigation, analysts used an aerial image to track a suspect past a private store camera, pinpointing the exact time the suspect passed the camera. Detectives then were able to view the subject's face in that private camera footage, use facial-recognition software to identify the individual, and apprehend him.").

316. *See Jones*, 565 U.S. at 416; Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018).

317. United States v. Tuggle, 4 F.4th 505, 524 (7th Cir. 2021) ("In those cases, the justices expressed concerns about surveillance leading to 'a precise, comprehensive record of a person's *public* movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.'" (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring))).

> movements," the cameras only highlighted Tuggle's *lack* of movement, surveying only the time he spent at home and thus not illuminating what occurred when he *moved* from his home.[318]

This public versus private distinction is true, as far as it goes, but misses the argument that the aggregation of personal details about Tuggle's home is quite revealing in itself. The same "familial, political, professional, religious, and sexual associations" identified as worthy of protection in public are equally revealing around a private home (and maybe more so).[319] Who you live with, what you wear, what you do, who you love, when you wake, party, pray, or exercise can all be uncovered by watching your activities around your house.[320] An unrestrained police power to monitor and record any activity, object, person, or pattern of movement around a home without a warrant likely goes beyond the ordinary expectations of homeowners in a free society.

In fact, under traditional Fourth Amendment analysis, the home usually benefits from a higher (if not the highest) level of constitutional protection.[321] What the Supreme Court was doing in *Jones* and *Carpenter* was extending the foundational protections/privacies of the home to public activities (which traditionally had not received the same protection).[322] The Supreme Court was not elevating the privacy of public activities over the privacy of home activities but trying to protect them as well. The *Tuggle* court inverted this traditional hierarchy, leaving long-term surveillance of a home less protected than long-term surveillance of movements in public.

The same error can be observed in evaluating the privacy invasion of retrospective digital searches. The *Tuggle* court appropriately identified the Supreme Court's concern with retrospective searches that give police a metaphorical time-machine-like power to review a person's life for incriminating activities.[323] But oddly, the *Tuggle* court ignored the activities

---

318. *Tuggle*, 4 F.4th at 524.

319. *See* Andrew Guthrie Ferguson, *Personal Curtilage: Fourth Amendment Security in Public*, 55 WM. & MARY L. Rev. 1283, 1309, 1313–22 (2014) (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)) (discussing the heightened protection of the area around a home).

320. *See* United States v. Dunn, 480 U.S. 294, 300 (1987) ("[In *Oliver*] we recognized that the Fourth Amendment protects the curtilage of a house and that the extent of the curtilage is determined by factors that bear upon whether an individual reasonably may expect that the area in question should be treated as the home itself." (citing Oliver v. United States, 466 U.S. 170, 180 (1984))); Tracey Maclin, Katz*,* Kyllo*, and Technology: Virtual Fourth Amendment Protection in the Twenty-First Century*, 72 MISS. L.J. 51, 63 (2002) ("*United States v. Dunn* elevated *Oliver*'s dicta on the meaning of curtilage to law." (footnote omitted)); *see also* California v. Ciraolo, 476 U.S. 207, 212–13 (1986) ("The protection afforded the curtilage is essentially a protection of families and personal privacy in an area intimately linked to the home, both physically and psychologically, where privacy expectations are most heightened.").

321. Stephanie M. Stern, *The Inviolate Home: Housing Exceptionalism in the Fourth Amendment*, 95 CORNELL L. REV. 905, 906–08 (2010).

322. *Jones*, 565 U.S. at 406, 413; Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

323. *Tuggle*, 4 F.4th at 525 ("[T]he [Riley] Court commented that '[h]istoric location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building,' essentially allowing the government to

around the home from the time-machine concern. The *Tuggle* court stated: "By the logic of *Riley* and *Carpenter*, . . . the pole camera surveillance here did not run afoul of the Fourth Amendment because the government could not 'travel back in time to retrace [Tuggle's] whereabouts' . . . ."[324] Again, this may be true but only important if Tuggle's public travels are more important than the privacies protected in and around the home. Police most certainly could (and did) travel back in time to retrace the defendant's incriminating (and personal) activities around his home.[325] Again, privileging public activities over home-based activities runs counter to the traditional hierarchy of Fourth Amendment protections.

To be fair, the *Tuggle* court acknowledged this tension. The court both articulated and then minimized the privacy intrusion of activities around the home:

> In one sense, the recordings painted a whole picture of the happenings outside Tuggle's front door by recording nonstop for eighteen months. In another important sense, however, the footage only depicted one small part of a much larger whole: Tuggle's life or the "whole of his physical movements." Given their immobile nature, the cameras could not make out an exhaustive record of Tuggle's "hitherto private routine," because much if not most of the relevant details occurred outside of the immediate area in front of Tuggle's home.[326]

Again, this argument minimizes the personal information that can be gained by watching a private home for months on end—monitoring which could reveal much of a person's life, including identifying friends, family, lovers, patterns, activities, habits, etc.[327] But, more fundamentally, it answers the wrong question. The Fourth Amendment search question has never turned on whether a technology exposed "the larger whole" of an individual's activities. The Supreme Court has never required that level of exposure.[328] *Katz* involved a few conversations.[329] *Kyllo* involved a particular night's thermal

---

go back in time." (second alteration in original) (quoting Riley v. California, 573 U.S. 373, 396 (2014))); *see id.* ("The advent of CSLI-like technology therefore allows the government to 'travel back in time to retrace a person's whereabouts,' obviating what would have been previous 'attempts to reconstruct a person's movements [that] were limited by a dearth of records and the frailties of recollection.'" (alteration in original) (quoting *Carpenter*, 138 S. Ct. at 2218)).

324. *Id.* (alteration in original) (quoting *Carpenter*, 138 S. Ct. at 2218).

325. *Id.* at 511–12.

326. *Id.* at 524–25 (citations omitted).

327. *Id.* ("[O]fficers [were] able to 'capture[] something not actually exposed to public view—the aggregate of all of [the defendant's] coming and going from the home, all of his visitors, all of his cars, all of their cars, and all of the types of packages or bags he carried and when.'" (alterations in original) (quoting State v. Jones, 903 N.W.2d 101, 111 (S.D. 2017))).

328. *See generally* Matthew Tokson, *Knowledge and Fourth Amendment Privacy*, 111 NW. U. L. REV. 139, 154–58 (2016) (discussing levels of information exposure and the Fourth Amendment).

329. Brief for Petitioner, Katz v. United States, 389 U.S. 347 (1967) (No. 35), 1967 WL 113605, at *5 ("The microphone was activated when Petitioner was a block away from the booth. The microphone was deactivated after Petitioner left the booth. Apparently, anybody could use the booth while the recording

reading.[330] *Jardines* involved a single sniff of a police dog.[331] *Knotts* involved a beeper's location.[332] None of these cases required a full exposure of personal information to be considered a search. Moreover, the warrantless monitoring in *Tuggle* was much more complete than any of those prior precedents. It would be like listening to all of Charlie Katz's phone calls or sniffing all the smells coming from Jolie Jardines's home (for eighteen months) and having the collected data available for retrospective access whenever police wished.[333]

Harder questions emerge as one goes through the rest of the Fourth Amendment factors. Is an always-on camera an enhancement or a superpower? The *Tuggle* court tried to have it both ways and got it wrong twice over. First, the *Tuggle* court relied on *Dow Chemical* for the proposition that visual enhancements do not change the Fourth Amendment analysis[334] and then on *Knotts* to claim that mere scientific or technological enhancements do not change the constitutional analysis.[335] Both cases are inapposite, with *Dow Chemical* specifically foreswearing any application to personal homes,[336] and

equipment was operative; in fact, on February 23, 1965, a stranger did use the booth and his conversation was recorded." (citations omitted)); Brief for Respondent, Katz v. United States, 389 U.S. 347 (1967) (No. 35), 1967 WL 1130636, at *3–4 ("Each day, as petitioner approached a certain spot about a block and a half away from the telephones, agents in a radio car surveilling petitioner signaled other agents near the booths, who then attached and activated the recorder and microphones. After petitioner departed, the device was removed.").

330. Brief for the United States, Kyllo v. United States, 533 U.S. 27 (2001) (No. 99-8508), 2000 WL 1890949, at *4 ("On January 16, 1992, between 3:30 and 4:00 a.m., Oregon National Guard Sergeant Dan Haas used an Agema 210 thermal imager to scan the triplex where Tova Shook and petitioner lived.").

331. Florida v. Jardines, 569 U.S. 1, 3–4, 11–12 (2013).

332. United States v. Knotts, 460 U.S. 276, 277 (1983) ("In this case, a beeper was placed in a five-gallon drum containing chloroform purchased by one of respondent's codefendants. By monitoring the progress of a car carrying the chloroform Minnesota law enforcement agents were able to trace the can of chloroform from its place of purchase in Minneapolis, Minn[esota], to respondent's secluded cabin near Shell Lake, Wis[consin].").

333. *See* Brief for Petitioner, Katz v. United States, 389 U.S. 347 (1967) (No. 35), 1967 WL 113605, at *4–6 (describing the facts of the case); Brief for Respondent, Katz v. United States, 389 U.S. 347 (1967) (No. 35), 1967 WL 1130636, at *2–4 (describing the facts of the case); *Jardines*, 569 U.S. at 3–5 (describing the facts of the case).

334. United States v. Tuggle, 4 F.4th 505, 515 (7th Cir. 2021) ("'[T]he mere fact that human vision is enhanced somewhat, at least to the degree here, does not give rise to constitutional problems' . . . ." (quoting Dow Chem. Co. v. United States, 476 U.S. 227, 238 (1986))).

335. *Id.* at 514 ("'[N]othing in the Fourth Amendment prohibit[s] the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in' certain instances." (citing *Knotts*, 460 U.S. at 282)).

336. The Court in *Dow* cautioned against extending the holding to a home. Apparently in *Dow*, the Government conceded (and the Supreme Court agreed) that the use of high aerial enhancements to view private property might require a different outcome. *See Dow Chem. Co.*, 476 U.S. at 238 ("It may well be, as the Government concedes, that surveillance of private property by using highly sophisticated surveillance equipment not generally available to the public, such as satellite technology, might be constitutionally proscribed absent a warrant.").

Knotts specifically stating that the beepers provided no enhancement that could not have been observed with the ordinary human eye.[337]

But even putting aside the misreading of precedent, the *Tuggle* court ignored its own reasoning. The *Tuggle* court admitted that the surveillance at issue went far beyond human capabilities—even enhanced human capabilities. This was not a team of officers with a camera but a sophisticated data collection system that did things no human could do with stored data.[338] More tellingly, the court rejected the government's argument that any technological enhancement of human capabilities is constitutional just because human officers could theoretically conduct similar surveillance. The court directly stated:

> We emphasize, however, that our decision in Tuggle's case does not rest on the premise that the government *could have*—in theory—obtained the same surveillance by stationing an agent atop the utility poles outside Tuggle's home, thus rendering the decision to instead use pole cameras constitutional. This fiction contravenes the Fourth Amendment and *Katz*'s command to assess reasonableness. To assume that the government would, or even could, allocate thousands of hours of labor and thousands of dollars to station agents atop three telephone poles to constantly monitor Tuggle's home for eighteen months defies the reasonable limits of human nature and finite resources. In our view, the premise that the government could realistically accomplish the pole camera surveillance here for more than a few days is a fiction that courts should not rely on to limit the Fourth Amendment's protections. We thus close the door on the notion that surveillance accomplished through technological means is constitutional simply because the government could theoretically accomplish the same surveillance—no matter how laborious—through some nontechnological means.[339]

In other words, always-on video cameras are doing something more than merely enhancing what a team of police officers could theoretically do if stationed to watch a home for eighteen months because such a team would be impossible to actually assemble (or remain unnoticed). Without quite admitting it, the *Tuggle* court recognized that police were relying on technological superpowers, not mere enhancements.

Finally, there is the admittedly ambiguous question of permeating surveillance. Always-on cameras are not permeating in the sense that a city-wide camera system (or PSS) might be. In *Tuggle*, the cameras were limited to a particular home, not spread out throughout the neighborhood.[340] Yet, the pervasive video streams offered deep and sustained invasions of personal

337. *Knotts*, 460 U.S. at 285 ("But there is no indication that the beeper was used in any way to reveal information as to the movement of the drum within the cabin, or in any way that would not have been visible to the naked eye from outside the cabin.").

338. *Tuggle*, 4 F.4th at 526.

339. *Id.* (citations omitted).

340. *Id.* at 511.

spaces and private property.[341] Again, as discussed before, the aggregation is of a different sort, not connecting locational data from different public places but connecting personal data from the same private place to other sources of police data. The surveillance is not broad but deep with cameras burrowing into the privacies around a home. The always-on cameras seep through the ordinary protections of physical obstructions, time, obscurity, and implicit licenses[342] to reveal things that would not be seen without the cameras.[343] While three cameras always watching you is not the same permeating system as thirty thousand cameras watching everyone, it is still an inescapable and fixed monitoring system.

The only factor that cuts against finding a Fourth Amendment search is the targeted nature of the monitoring. Tuggle was justifiably suspected of criminal wrongdoing, so the use of invasive monitoring was not arbitrary (in the sense of random). But even that factor is not without complication.

First, suspicion, alone, does not obviate a warrant requirement. In both *Jones* and *Carpenter*, police (correctly) suspected the defendants were up to no good, but police still violated their expectation of privacy by tracking them without a warrant.[344] The targeted nature of the surveillance did not cure the constitutional violation. In fact, targeted surveillance *without a warrant* may be just as problematic as overbroad arbitrary surveillance. Police using unrestrained and invasive governmental power against disfavored individuals without going through the normal process to get judicial approval may be more threatening to liberty.[345]

---

341. To support the depth argument, the Supreme Court in *Riley* also used the term "pervasive" to describe the deep dive into the smartphone. Again, this was not a broad search as much as a deep search into a particular phone and a particular individual's private life. *See* Riley v. California, 573 U.S. 373, 395 (2014) ("[T]here is an element of *pervasiveness* that characterizes cell phones but not physical records. Prior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day." (emphasis added)).

342. Florida v. Jardines, 569 U.S. 1, 8 (2013) (discussing the "implicit licenses" that protect private property from physical intrusion by investigative agents).

343. *Id.* at 12 (Kagan, J., concurring) ("For me, a simple analogy clinches this case—and does so on privacy as well as property grounds. A stranger comes to the front door of your home carrying super-high-powered binoculars. He doesn't knock or say hello. Instead, he stands on the porch and uses the binoculars to peer through your windows, into your home's furthest corners. It doesn't take long (the binoculars are really very fine): In just a couple of minutes, his uncommon behavior allows him to learn details of your life you disclose to no one. Has your 'visitor' trespassed on your property, exceeding the license you have granted to members of the public to, say, drop off the mail or distribute campaign flyers? Yes, he has. And has he also invaded your 'reasonable expectation of privacy,' by nosing into intimacies you sensibly thought protected from disclosure? Yes, of course, he has done that too." (quoting Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring))).

344. In almost all cases, police have some suspicion of a suspect. The suspicion does not remove the need to follow constitutional and procedural requirements; in fact, it is the predicate for following such rules.

345. That is why the Founders required warrants for targets of governmental police power. *See, e.g.*, Thompson v. Louisiana, 469 U.S. 17, 20 (1984) (per curiam) ("[W]e have consistently reaffirmed our understanding that in all cases outside the exceptions to the warrant requirement the Fourth Amendment requires the interposition of a neutral and detached magistrate between the police and the 'persons, houses, papers, and effects' of citizens.").

In this sense, "arbitrary" has another meaning, namely the use of government power was without a set process or limits. The Founders' fear of general warrants was not just that police powers would be used against everyone but also that search powers could be used against people like themselves who the government wished to monitor.[346] Police invasions of privacy and security (without judicial approval) were harmful because the power might be wielded in an abusive fashion against people suspected of wrongdoing (such as those critiquing the government). This fear of arbitrary police power undermined the right to be secure protected by the Fourth Amendment.

In sum, if an expectation of privacy from persistent surveillance technologies lives on a continuum, what do we make of the *Tuggle* decision? Most of the factors cut in favor of finding a reasonable expectation of privacy and thus a Fourth Amendment violation. So why did the court in *Tuggle* come out the other way? I submit that in addition to failing to examine the legal clues set out in Supreme Court precedent, the court also failed to understand the systems nature of the surveillance at issue. As discussed earlier, seeing the unit of surveillance of the pole cameras as also including networked backend, searchable databases makes it more likely that the long-term pole cameras violated a reasonable expectation of privacy.

CONCLUSION

Courts are looking to solve the puzzle of persistent surveillance technologies. This Article offers a roadmap for future cases. In three steps, courts can address and justify a new approach to a growing threat to privacy.

First, courts must convince themselves that the act of persistent surveillance is different enough from traditional surveillance techniques to warrant a new analysis. Acknowledging the six A's of (1) automation, (2) acceleration, (3) accuracy, (4) accumulation, (5) aggregation, and (6) actualization common to all digital persistent surveillance technologies reveals a different act and thus justifies a different Fourth Amendment approach unencumbered by analog precedent.

Second, courts must recognize that questions about persistent surveillance cannot be answered without accurately defining the unit of surveillance to be examined. Some persistent surveillance technologies are systems and some are tools. Systems are more likely to violate expectations of privacy but defining what the technology is remains a contested choice. Similarly, courts must decide whether to examine the potential privacy threat of interconnected and easily

346. Tomkovicz, *supra* note 205, at 1134 ("The Framers objected to general warrants and writs of assistance because they resulted in arbitrary deprivations of privacy, property, and liberty. Those deprivations were arbitrary in part because officers were authorized to search and seize upon bare suspicion. They were also arbitrary and dangerous because agents of the executive were given 'unlimited discretion' to choose whom, where, and what to search and seize." (footnotes omitted)).

updateable surveillance systems or examine the actual collection in any particular case. This choice between capacity and actuality is also contested with hard questions about the role of courts, the dangers of evolving technologies, and fact-bound determinations all at play.

Finally, courts must analyze the clues provided by the Supreme Court about when certain forms of surveillance violate a reasonable expectation of privacy. The questions framed in Part II offer guideposts for analysis, recognizing that the answer lies somewhere along a continuum. Persistent surveillance technologies that are digital, aggregated, retrospective, arbitrary, permeating, and that give superpowers which impact associational freedoms will likely violate a reasonable expectation of privacy if used without a warrant.

As discussed, both the Baltimore surveillance planes and the long-term pole cameras offer good examples about how this three-step analysis, properly applied, can answer difficult questions about Fourth Amendment freedoms. As the Supreme Court has recognized, new technologies do threaten long-standing Fourth Amendment values, and courts need to keep up. This Article has sought to clarify a way forward, applying existing Fourth Amendment insights to create a framework for future challenges arising from growing persistent surveillance threats.