EMORY | LAW

Emory Law Journal

Volume 66
Issue 3 *The 2016 Randolph W. Thrower Symposium — Redefined National Security Threats: Tensions and Legal Implications*

Article 4

2017

Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public

Rachel Levinson-Waldman

HIDING IN PLAIN SIGHT: A FOURTH AMENDMENT FRAMEWORK FOR ANALYZING GOVERNMENT SURVEILLANCE IN PUBLIC

Rachel Levinson-Waldman[*]

INTRODUCTION

Over the last several decades, the range and capabilities of easily available technologies have expanded at an astonishing pace. The beeper gave way to the flip phone, which has largely been replaced by the "smartphone," a mini-computer that fits in the palm of your hand and is more powerful than the desktop machine of the 1980s.[1] Paper maps are increasingly rare, replaced by built-in Global Positioning System (GPS) devices or the ubiquitous smartphone. The days of having to keep change in a glove compartment to pay a toll attendant are long past; instead, an EZ-Pass reader enables drivers to travel seamlessly across multiple states and pay the charges directly from an online account.

These and other technologies, which are valuable to civilians and law enforcement alike, also enable a granular view of citizens' movements and associations in public over long periods of time at a relatively cheap cost. The 2002 movie *Minority Report*,[2] which seemed wildly futuristic at the time, effectively predicted many of the technologies now available to police at the

[*] Rachel Levinson-Waldman is Senior Counsel to the Liberty and National Security Program at the Brennan Center for Justice. This has been a multi-year project; I began working on this paper while I was pregnant with my second child and he can now ride a scooter. I therefore owe numerous debts of gratitude. For countless conversations and feedback on drafts, I am grateful to my current and former Brennan Center colleagues Liza Goitein, Faiza Patel, Michael Price, Michael German, and Amos Toh. For extremely able research assistance, I am grateful to Erica Posey, Andrew Lindsay, Brynne O'Neal, Jeremy Carp, Patricia Stottlemyer, Andrew Lehmann, Andrew Nellis, and Charlotte Lunday. For participating in discussions and roundtable meetings and offering comments on drafts, I am grateful to Marc Blitz, Danielle Citron, David Cole, Laura Donohue, Joshua Dratel, Hanni Fakhoury, Harley Geiger, Marcia Hofmann, Margaret Hu, Orin Kerr, David Lipson, David Robinson, Julian Sanchez, Stephen Schulhofer, Nick Selby, Christopher Slobogin, Jay Stanley, Amie Stepanovich, Daniel Weitzner, Nathan Wessler, Ben Wizner, and Harlan Yu. Finally, I wish to thank the *Emory Law Journal*, in particular Nathan North and Grace Zoller for their fine editing and Katya Keremidchieva and Mary Grace Gallagher for their excellent work on the February 2016 symposium.

[1] *See* John Sheesley, *The 80's Supercomputer that's Sitting in Your Lap*, TECHREPUBLIC (Oct. 13, 2008, 8:47 AM), http://www.techrepublic.com/blog/classics-rock/the-80s-supercomputer-thats-sitting-in-your-lap/.

[2] MINORITY REPORT (20th Century Fox 2002).

click of a button: drones, facial recognition scanners, vehicle trackers, and more.[3]

Where law enforcement is involved, these powerful new technologies also raise questions about how their use can be harmonized with the U.S. Constitution. The Fourth Amendment guarantees "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[4] Under what circumstances does an eye in the sky (or on a pole, or inside your phone) constitute a search under the Fourth Amendment—and thus presumptively require a warrant—when it is used for public surveillance?

It seems inconceivable that the Founders, who could fairly be described as obsessed with Americans' right to be let alone, could have envisioned, let alone endorsed, the degree and depth of intrusion into individuals' lives that is enabled by present-day surveillance technologies.[5] At the same time, it is notoriously difficult to articulate when surveillance in public works a constitutional violation and when it is simply the price for leaving the house. While the judiciary is nowhere near consensus, courts are finding that some public manifestations of this new, digitally-enabled tracking are so inimical to any standard notions of privacy that the Fourth Amendment imposes limits on their use, as discussed in further detail below.

The home has always been sacrosanct territory for the Fourth Amendment. In the late 1960s, the Supreme Court began to expand its conceptions of the Fourth Amendment's protections beyond the doorstep. In *United States v. Katz*, involving a payphone (then a cutting-edge technology), the Court laid the groundwork for a doctrine holding that the Fourth Amendment protects individuals from police intrusion when the intrusion violates a "reasonable expectation of privacy."[6] A couple of decades later, the Supreme Court confronted another novel technology, which police were using to tail criminal suspects: the beeper.

---

[3] *See* Michael Casey, *Facial Recognition Software Is Scanning You Where You Least Expect It*, CBS NEWS (June 25, 2015, 6:00 AM), http://www.cbsnews.com/news/facial-recognition-software-is-scanning-you-where-you-least-expect-it/; *Drones & MiniDrones*, BROOKSTONE, http://www.brookstone.com/drones-minidrones (last visited Mar. 16, 2016); Jeremy Scahill & Margot Williams, *Stingrays: A Secret Catalogue of Government Gear for Spying on Your Cellphone*, INTERCEPT (Dec. 17, 2015, 12:23 PM), https://theintercept.com/2015/12/17/a-secret-catalogue-of-government-gear-for-spying-on-your-cellphone/.

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

[5] *See* Thomas K. Clancy, *The Framers' Intent: John Adams, His Era, and the Fourth Amendment*, 86 IND. L.J. 979, 989–991 (2011).

[6] 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

In two key Supreme Court cases, police officers planted beeper devices in suspects' cars and used their signals to follow the car when a close physical tail was impractical or would have revealed the surveillance.[7] In these cases, the Court concluded that because the police could have freely followed and observed the suspects on public roads and highways without getting a warrant, using a beeper to make the job a little easier did not sound constitutional alarms.[8] Although the Court warned that its analysis might not hold if the police undertook dragnet surveillance, its reasoning has long been used as support for the broad proposition that there is no reasonable expectation of privacy in one's movements in public space.[9]

Of course, the stock-in-trade of good policing often involves the real-time observation of people going about their daily business. This kind of visual observation, while potentially intrusive or discomfiting to the subject or passersby, does not raise constitutional issues.[10] It is also, however, cost- and resource-intensive.[11] These costs have historically required law enforcement agencies to make critical judgments about what types of police work and surveillance to undertake, and they have acted as an effective brake on at least some kinds of government overreach. Practical limitations on government surveillance in public offered "structural privacy," privacy arising not from legislative or judicial decisionmaking, but from the physical and technical limitations on carrying out long-term, wide-range surveillance of multiple persons or areas.[12]

Enter digital technology. As surveillance techniques grow ever more technologically sophisticated, the quantum of data that is easily available grows as well, while the cost of obtaining, keeping, and analyzing it generally drops. At the same time, "our historical expectations of privacy do not change or somehow weaken simply because we now happen to use modern technology to engage in activities in which we have historically maintained protected privacy

---

[7] *See, e.g.*, United States v. Karo, 468 U.S. 705, 707 (1984) (considering the constitutionality of using a beeper for surveillance); United States v. Knotts, 460 U.S. 276, 277 (1983) (considering the constitutionality of using a concealed beeper to trace a can of chloroform from its place of purchase to a secluded cabin).

[8] *Karo*, 468 U.S. at 721; *Knotts*, 460 U.S. at 285.

[9] *See, e.g.*, United States v. Cuevas-Perez, 640 F.3d 272, 273–74 (7th Cir. 2011), *vacated and remanded*, 565 U.S. 1189 (2012); Christensen v. Cty. of Boone, 483 F.3d 454, 460 (7th Cir. 2007); United States v. Walker, 771 F. Supp. 2d 803, 810 (W.D. Mich. 2011).

[10] *Knotts*, 460 U.S. at 281.

[11] United States v. Jones, 565 U.S. 400, 429–30 (2012) (Alito, J., concurring in the judgment) (discussing the costs and burdens of traditional surveillance methods).

[12] *See* Harry Surden, *Structural Rights in Privacy*, 60 SMU L. REV. 1605, 1607–08 (2007).

interests."[13] How, then, is the judiciary "to adapt traditional Fourth Amendment concepts to the Government's modern, more sophisticated investigative tools"?[14]

This Article proposes one way to meet this challenge. Existing case law, seen through a new lens, provides the blueprint for a workable, comprehensive mechanism for applying the Fourth Amendment to digital age public surveillance technologies.[15] This approach aggregates factors courts have already identified as relevant to their Fourth Amendment analysis, but in an ad hoc manner, and transforms them into a more rigorous, replicable approach.

These factors are: (1) the duration of the surveillance; (2) the lowering of structural barriers to pervasive surveillance, reflected in the greatly reduced cost of tracking; (3) the recording of an individual's or group's movements; (4) the elicitation of information from within a protected space such as a home; and, as appropriate, (5) whether the technology undermines core constitutional rights and (6) whether surveillance technologies are piggy-backed on each other. Pulling out and articulating these factors, and analyzing how and why they should be considered, seeks to add rigor to the improvisatory method that has defined the judiciary's consideration of these questions.

Once the Fourth Amendment is triggered, the Constitution generally requires police to get a warrant, which must meet the particularity standard.[16] That will usually be possible through careful *ex ante* and *ex post* tailoring; where it is not, that use of the surveillance technology may not be compatible with the Constitution. In addition, courts must be alert to attempts to justify a wide swath of surveillance activities on the grounds that they satisfy a "special need," an exception to the warrant requirement that could quickly swallow the rule.[17]

---

[13] United States v. Davis, 785 F.3d 498, 524–25 (11th Cir. 2015) (Rosenbaum, J., concurring).

[14] United States v. Ganias, 755 F.3d 125, 134 (2d Cir. 2014), *reh'g en banc granted*, 791 F.3d 290 (2d Cir. 2015), *rev'd in part*, 824 F.3d 199 (2d Cir. 2016) (en banc).

[15] There are other mechanisms for approaching surveillance reform as well. Most notably, Christopher Slobogin has proposed practical legislative methods and offered the theoretical and conceptual underpinnings for doing so, including shifting to an administrative law rather than constitutional law framework. CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT (2007); Christopher Slobogin, *Policing as Administration*, 165 U. PA. L. REV. 91 (2016). This piece does not take a position on those proposals, which are also worth serious attention.

[16] U.S. CONST. amend. IV ("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." (emphasis added)).

[17] Griffin v. Wisconsin, 483 U.S. 868, 873 (1987) (observing that the Court has permitted exceptions to the warrant requirement "when 'special needs, beyond the normal need for law enforcement, make the warrant

* * *

This Article proceeds as follows: Part I provides a brief overview of the courts' evolution on the Fourth Amendment implications of surveillance in the public space, from initial hints that dragnet surveillance might be problematic to growing recognition that modern methods of information capture and public space surveillance pose privacy concerns of constitutional magnitude. Part II outlines a new, multi-factor approach for both courts and law enforcement to use in assessing whether the Fourth Amendment is implicated by surveillance in public, drawing on existing case law and various scholarly approaches. It assesses how a warrant for surveillance in public can meet the Fourth Amendment's particularity standard and explores why the special needs exception to the warrant requirement will rarely come into play. It also briefly addresses the circumstances in which the First Amendment and Fourteenth Amendment may provide avenues for relief. Finally, Part III uses several case studies to explore how this approach plays out in the context of specific technologies that facilitate surveillance in public.

I. SURVEILLANCE TECHNOLOGIES AND THE COURTS

This section comprises two main parts. First, it briefly reviews the early stages of the Supreme Court's modern privacy jurisprudence, starting with the Court's seminal 1967 decision in *United States v. Katz*.[18] Second, it canvasses both the technology behind and the current legal treatment of seven major surveillance tools: GPS automobile tracking, cellular phones, video surveillance cameras, drones, license plate readers, body-worn cameras, and biometric identification technologies. In doing so, it demonstrates that the era of "dragnet-type law enforcement practices," about which the Supreme Court warned in *United States v. Knotts*, has come to pass.[19]

A. The Supreme Court's Early Privacy Jurisprudence

The Supreme Court launched its modern privacy jurisprudence in 1967, with *United States v. Katz*.[20] Trying to catch Charles Katz in the act of placing an illegal bet, the Federal Bureau of Investigation (FBI) used a wiretap to listen in

and probable-cause requirement impracticable'" (quoting New Jersey v. T.L.O., 469 U.S. 325, 351 (1985) (Blackmun, J., concurring in judgment))).

[18] 389 U.S. 347 (1967).

[19] 460 U.S. 276, 284 (1983).

[20] 389 U.S. at 359.

on a call he made from a public pay phone booth.[21] The agents did not get a warrant for the wiretap, reasoning that because the pay phone was in public and Katz could be seen through its glass walls, he was taking the risk that someone might overhear the conversation.[22] In other words, because a member of the public could listen in, so could the police.

The Supreme Court saw it differently. The Court rejected its previous, crabbed reading of the Constitution, which had held that the Fourth Amendment protected only private spaces, such as homes, and only against physical intrusion.[23] In Justice Stewart's ringing words in *Katz*, "the Fourth Amendment protects people, not places."[24] Thus, "what [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[25] The fact that Katz had shut the telephone booth door showed his intent to keep the conversation private.

Katz established for the first time that individuals had rights to privacy that were not dependent on whether a physical locale had been breached. In an influential concurrence, Justice Harlan set out a two-prong test inquiring into an individual's "reasonable expectation of privacy": first, does that individual have a subjective expectation of privacy in a particular activity? And second, if so, is society prepared to recognize that expectation as reasonable?[26]

As the Supreme Court continued to hear challenges to law enforcement's use of surveillance and tracking technologies in public, it built on Harlan's formulation, inquiring into both the subjective expectation of privacy and society's acceptance of that expectation. At the same time, the Court absorbed Harlan's caveat that while the Constitution "protects people, not places," the process of determining the scope of that protection "requires reference to a 'place.'"[27] As a result, courts were initially relatively dismissive of claims for privacy in public spaces,[28] focusing instead on the moment when surveillance

---

[21] *Id.* at 348.

[22] *Id.* at 352.

[23] *See* Goldman v. United States, 316 U.S. 129, 135 (1942); Olmstead v. United States, 277 U.S. 438, 463–66 (1928).

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

[25] *Id.* at 351–52.

[26] *Id.* at 361 (Harlan, J., concurring).

[27] *Id.*

[28] *See, e.g.*, United States v. Knotts, 460 U.S. 276, 281 (1983) ("A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."); United States v. Gonzalez, 328 F.3d 543, 548 (9th Cir. 2003) (no reasonable expectation of privacy in a hospital mailroom open to the public).

strays into a private home[29] or its curtilage,[30] or, in some circumstances, a private office[31] or locker room.[32]

In *United States v. Knotts*, for example, the Court upheld the police's warrantless use of a hidden beeper to track a suspect's car down public roads.[33] Because anyone on the roads could see the driver, he had no legitimate expectation of privacy in his movements.[34] By contrast, the Court ruled the following year that when a beeper is taken inside a private home and reveals information that otherwise would have required a warrant to obtain, it is a search.[35]

Compared to today's technology, however, the beeper was practically primitive. While it allowed law enforcement to do relatively precise tracking and to locate a person or item out of direct eyesight, it still required constant attention.[36] If the officer or agent lost the beeper's position, he would have to return to its last known location and attempt to find it manually via radio receiver.[37] The *Knotts* majority presciently observed that compared to this painstaking, resource-intensive, individualized surveillance, "dragnet-type law enforcement practices" could change the Fourth Amendment calculus.[38]

---

[29] *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 34 (2001) ("We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area' constitutes a search . . . ." (citation omitted)); United States v. Karo, 468 U.S. 705, 713 (1984) (holding that the monitoring of a beeper inside a private home raised constitutional concerns).

[30] *See, e.g.*, Florida v. Jardines, 133 S. Ct. 1409, 1414 (2013) ("We therefore regard the area 'immediately surrounding and associated with the home'—what our cases call the curtilage—as 'part of the home itself for Fourth Amendment purposes.'").

[31] *See, e.g.*, O'Rourke v. Hayes, 378 F.3d 1201, 1206 (11th Cir. 2004) ("Offices and other workplaces are among the areas in which individuals may enjoy . . . a reasonable expectation of privacy."); Richards v. Cty. of Los Angeles, 775 F. Supp. 2d 1176, 1185–86 (C.D. Cal. 2011) (surreptitious video recording of a "dispatch" room shared by public employees violated Fourth Amendment).

[32] *See, e.g.*, Brannum v. Overton Cty. Sch. Bd., 516 F.3d 489, 496–97 (6th Cir. 2008) (videotaping students in a school locker room violates reasonable expectation of privacy).

[33] 460 U.S. at 285.

[34] *Id.*

[35] United States v. Karo, 468 U.S 705, 716–17 (1984).

[36] *See* Richard H. McAdams, Note, *Tying Privacy in* Knotts*: Beeper Monitoring and Collective Fourth Amendment Rights*, 71 VA. L. REV. 297, 314 (1985) ("[B]eepers require continued observation to discover someone's identity, route, and final destination.").

[37] *Knotts*, 460 U.S. at 277 (describing beepers as "radio transmitter[s], usually battery operated, which emit[] periodic signals that can be picked up by a radio receiver").

[38] *Id.* at 284; *see also* People v. Weaver, 909 N.E.2d 1195, 1200 (N.Y. 2009) (noting that *Knotts* reserved the question of "twenty-four hour surveillance of any citizen" for another day, and observing that "26 years after *Knotts*, GPS technology, even in its present state of evolution, quite simply and matter-of-factly forces the issue").

B. Courts and Modern Surveillance Technologies: A Brief Overview

These practices are upon us. They represent a new era in sophistication and in the government's ability to track individuals' locations, activities, and associations via public space surveillance, often at a fraction of the cost it would take for individual officers to do the job. And they require a new approach to ensure that an individual "does not leave his privacy behind when he walks out his front door."[39] This section provides a brief overview of the public tracking and surveillance technologies that are now commonly known to be in law enforcement's hands and an outline of the current doctrinal landscape.

1. GPS Automobile Tracking

GPS devices use satellites to calculate their location with precision.[40] While making car trips easier and faster, they also enable law enforcement agencies to track vehicles.[41] Standalone GPS units can be surreptitiously attached to cars,[42] or the police can get access to data from built-in devices.[43] Once attached, a GPS device reports the location of the vehicle with precision and in real time.[44] GPS devices are also used in cell phones to help calculate location for a variety of purposes.[45]

From relatively early on, courts have recognized that GPS allows for precise tracking on a monumental scale. In 2009, for instance, New York's highest court considered the warrantless use of a GPS device to monitor a car's location for sixty-five days, observing:

> GPS is not a mere enhancement of human sensory capacity, it facilitates a new technological perception of the world in which the

---

[39] United States v. Maynard, 615 F.3d 544, 563 (D.C. Cir. 2010).

[40] *See How Does GPS Work?*, PHYSICS.ORG, www.physics.org/article-questions.asp?id=55 (last visited Aug. 17, 2015).

[41] *See id.*

[42] *See, e.g.*, Alyson Sheppard, *Police Shoot Cars with GPS Tags to Reduce High-Speed Chases*, POPULAR MECHANICS (Nov. 6, 2013), http://www.popularmechanics.com/technology/military/news/police-shoot-cars-with-gps-tags-to-reduce-high-speed-chases-16127245.

[43] *See, e.g.*, Ben Wojdyla, *Your Car* Is *Spying on You—But Whom Is It Spying For?*, POPULAR MECHANICS (Feb. 21, 2012), http://www.popularmechanics.com/cars/how-to/a7469/your-car-is-spying-on-you-but-whom-is-it-spying-for/.

[44] THE CONSTITUTION PROJECT, LIBERTY AND SECURITY COMMITTEE STATEMENT ON LOCATION TRACKING 3 (2011), http://www.constitutionproject.org/pdf/LocationTrackingReport.pdf; *see also* Sheppard, *supra* note 42 ("Once the suspect's car is tagged, the GPS module relays the car's coordinates, heading, and speed every 3 to 5 seconds to police dispatch.").

[45] *See The Problem with Mobile Phones*, ELEC. FRONTIER FOUND., https://ssd.eff.org/en/module/problem-mobile-phones (last updated Feb. 10, 2015).

> situation of any object may be followed and exhaustively recorded over, in most cases, a practically unlimited period. The potential for a similar capture of information or "seeing" by law enforcement would require, at a minimum, millions of additional police officers and cameras on every street lamp.[46]

These implications for privacy made it "clear" that "the great popularity of GPS technology for its many useful applications may not be taken simply as a massive, undifferentiated concession of personal privacy to agents of the state."[47] Because the technology enabled law enforcement to "track[] and record[] relentlessly" the defendant for over two months, the surveillance violated the state constitution's "prohibition against unreasonable searches."[48]

Several years later, the Supreme Court was confronted with a similar case. In *United States v. Jones*, the FBI attached a GPS tracker to a suspected drug dealer's car without a valid warrant.[49] The device relayed the car's location with near-precision for a month, ultimately sending over 2000 pages of data via cell phone to a government computer.[50] The plurality ruled narrowly, holding that the physical attachment of the tracker to Jones's property was a trespass, and was thus an unconstitutional search.[51] In two concurring opinions, however, five members of the Court highlighted the privacy concerns raised by location tracking, emphasizing the length of the surveillance, the low cost and surreptitious nature, and the unmatched intrusiveness.[52]

Only one court so far has addressed whether using a built-in GPS device without a warrant would constitute a search. In *United States v. Williams*, a federal district court in Kentucky ruled that activating an in-car GPS device to locate a vehicle did not violate the Fourth Amendment, but the court highlighted

---

[46] People v. Weaver, 909 N.E.2d 1195, 1199 (N.Y. 2009).

[47] *Id.* at 1200.

[48] *Id.* at 1203.

[49] 565 U.S. 400, 403 (2012).

[50] *Id.*

[51] *Id.* at 404–05.

[52] *See id.* at 415–16 (Sotomayor, J., concurring) ("GPS monitoring generates 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. . . . [B]ecause GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices . . . ."); *id.* at 430 (Alito, J., concurring) ("[T]he use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy. For such offenses, 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.").

the fact that the device was used only to identify the location at a discrete moment in time, not to "monitor" the vehicle's movements.[53]

2. Cellular Phones

Some 90% of Americans regularly carry a cell phone, using it to make phone calls, to send texts, and, for the 64% who use a smartphone, to go online, find directions, play games, and more.[54] These cell phones also effectively serve as personal tracking devices. When turned on, they constantly report their location to their cellular service provider, and service providers typically store that location data, at least temporarily.[55] The proliferation of cell towers means that the precision of cell phone targeting is increasing exponentially, perhaps to a point of even greater precision than GPS data.[56] In addition to accessing this wealth of real-time data, law enforcement may also compel service providers and other third parties to hand over records of individuals' locations going back months.[57]

Other technologies come into play as well. Smartphones equipped with Wi-Fi and Bluetooth technology continuously send out signals with identifying information to establish connections; any receiver can determine which phone

---

[53] 2015 WL 4484060, at *5–6 (W.D. Ky. July 22, 2015).

[54] *Mobile Technology Fact Sheet*, PEW RESEARCH CTR. (Dec. 27, 2013) http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/.

[55] *Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy: Hearing Before the Subcomm. on Privacy, Tech. & the Law of the S. Comm. on the Judiciary*, 112th Cong. 228 (2011) (statement of the ACLU), https://www.aclu.org/files/assets/senate_hearing_mobile_tracking_may_2011_-_final.pdf (noting that location data is recorded "approximately every seven seconds"); *Cell Phone Location Tracking Request Response—Cell Phone Company Data Retention Chart*, ACLU, https://www.aclu.org/cell-phone-location-tracking-request-response-cell-phone-company-data-retention-chart (last visited Apr. 13, 2014) (listing data retention times for different service providers).

[56] *See Geolocational Privacy and Surveillance (GPS) Act: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Sec. of the H. Comm. on the Judiciary*, 112th Cong. 6–20 (2012) (statement of Matt Blaze), http://www.crypto.com/papers/blaze-gps-20120517.pdf; Andy Greenberg, *Reminder to Congress: Cops' Cellphone Tracking Can Be Even More Precise Than GPS*, FORBES (May 17, 2012, 1:57 PM), http://www.forbes.com/sites/andygreenberg/2012/05/17/reminder-to-congress-cops-cellphone-tracking-can-be-even-more-precise-than-gps/#578e3957263c; *see also In re* Application for Tel. Info. Needed for a Criminal Investigation, 119 F. Supp. 3d 1011, 1023 (N.D. Cal. 2015) ("Cell phones generate far more location data [than car GPS systems] because, unlike the vehicle in *Jones*, cell phones typically accompany the user wherever she goes.").

[57] *See, e.g.*, United States v. Carpenter, 819 F.3d 880, 895 (6th Cir. 2016) (case involving 215 days of cell-site location information); United States v. Graham, 824 F.3d 421, 441 (4th Cir. 2016) (en banc) (Wynn, J., dissenting in part and concurring in part) (case involving 221 days of cell-site location information); *see also* Patrick T. Chamberlain, Note, *Court Ordered Disclosure of Historical Cell Site Location Information: The Argument for a Probable Cause Standard*, 66 WASH. & LEE L. REV. 1745, 1747–48 (2009).

is where at any given time, and how long it has been there.[58] Phones can also determine their locations via GPS satellites.[59] The phone's location history is stored on the device until the user clears it and turns off location tracking.[60] In the meantime, third party applications can request access to that location data,[61] which can be transmitted without the user's direct interaction.[62]

In addition, as of late 2014, nearly fifty state and local police departments in the United States were known to be using a device popularly called a Stingray to directly intercept all cell phone signals in a given area.[63] Stingrays pretend to be cell towers, forcing all cell phones in their vicinity to connect through them and reveal at least their approximate location, even without making a call.[64] Notably, they work only when the cell phone is *not* in use—that is, precisely when the average user would have no reason to believe his location could be revealed.[65] Newer technology also allows law enforcement to locate cell phones by "passively" receiving the radio waves the phones emit when they connect through a cell tower.[66]

Not only are phones pervasive, but unlike cars, they go nearly everywhere.[67] As one court observed, they are the "easiest means to gather the most comprehensive data about a person's public—and *private*—movements

---

[58] *The Problem with Mobile Phones*, *supra* note 45.

[59] *Id.*; *see also* Stephanie Lockwood, Note, *Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators*, 18 HARV. J.L. & TECH. 307, 308 (2004).

[60] *See* Lisa Eadicicco, *Use This Trick to See a Map of Everywhere Your iPhone Knows You've Been*, BUS. INSIDER (Apr. 1, 2015, 9:31 AM), http://www.businessinsider.com/how-to-see-location-history-iphone-2015-4.

[61] *The Problem with Mobile Phones*, *supra* note 45.

[62] *See In re* Application for Tel. Info. Needed for a Criminal Investigation, 119 F. Supp. 3d 1011, 1014 (N.D. Cal. 2015) ("Additionally, most modern smartphones have applications that continually run in the background, sending and receiving data without a user having to interact with the cell phone.").

[63] Kate Klonick, *Stingrays: Not Just for Feds!*, SLATE (Nov. 10, 2014, 9:52 AM), http://www.slate.com/articles/technology/future_tense/2014/11/stingrays_imsi_catchers_how_local_law_enforcement_uses_an_invasive_surveillance.single.html; *see also* John Kelly, *Cellphone Data Spying: It's Not Just the NSA*, USA TODAY (Dec. 8, 2013), http://www.usatoday.com/story/news/nation/2013/12/08/cellphone-data-spying-nsa-police/3902809/.

[64] Klonick, *supra* note 63.

[65] *See* State v. Andrews, 134 A.3d 324, 352 (Md. Ct. Spec. App. 2016).

[66] Jennifer Valentino-DeVries, *Police Snap Up Cheap Cellphone Trackers*, WALL ST. J. (Aug. 18, 2015, 12:57 PM), http://www.wsj.com/articles/police-snap-up-cheap-cellphone-trackers-1439933271.

[67] Riley v. California, 134 S. Ct. 2473, 2490 (2014) ("According to one poll, nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower.").

available."[68] It is thus no surprise that a majority of lower courts have held that acquiring real-time location information via cell phone tracking, particularly for more than a few days, requires probable cause and a search warrant.[69] At least

---

[68] United States v. Powell, 943 F. Supp. 2d 759, 780 (E.D. Mich. 2013); *see also Riley*, 134 S. Ct. at 2490 (observing cell phone records "can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building").

[69] *See, e.g.*, United States v. Johnson, No. 1:15-CR-90-01, 2015 WL 5918741, at *2 (W.D. Mich. Oct. 9, 2015) (noting, without discussion, that a warrant had been requested and granted to initiate real-time cellular phone tracking); *In re* Application of the U.S. for an Order Authorizing (1) Installation & Use of a Pen Register & Trap & Trace Device or Process, (2) Access to Customer Records, & (3) Cell Phone Tracking, 441 F. Supp. 2d 816, 837 (S.D. Tex. 2006) ("[D]etailed location information, such as triangulation and GPS data, . . . unquestionably implicate Fourth Amendment privacy rights."); *In re* Application of the U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., 2006 U.S. Dist. LEXIS 11747, at *2 (S.D.N.Y. Feb. 28, 2006); *In re* Application of the U.S. for an Order Authorizing the Disclosure of Prospective Cell Site Info., 412 F. Supp. 2d 947, 949–50 (E.D. Wis. 2006); *In re* Application of the U.S. for an Order Authorizing Installation & Use of a Pen Register & a Caller Identification Sys. on Tel. Nos. [Sealed], 402 F. Supp. 2d 597, 605 (D. Md. 2005); *In re* Applications of U.S. for Orders Authorizing Disclosure of Cell Site Info., Nos. 05-403, 05-404, 05-407, 05-408, 05-409, 05-410, 05-411, 2005 WL 3658531, at *1 (D.D.C. Oct. 26, 2005); *In re* Application of the U.S. for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device & (2) Authorizing Release of Subscriber Info. and/or Cell Site Info., 384 F. Supp. 2d 562, 564 (E.D.N.Y. 2005); *cf. In re* Application of the U.S. for an Order: (1) Authorizing Installation & Use of a Pen Register & Trap & Trace Device; (2) Authorizing Release of Subscriber & Other Info.; and (3) Authorizing Disclosure of Location-Based Servs., No. 07-128, 2007 WL 3342243, at *1 (S.D. Tex. Nov. 7, 2007) (holding that no showing of probable cause is required "when the Government seeks real-time cell site data" but to obtain real-time "'Enhanced 911' services" the government must show probable cause because there is no question it is being used to establish the exact location of a person or device). Surveys have also reflected this sentiment, with cell phone users expressing concerns about tracking and attempting to take precautions to block such monitoring. *See, e.g.*, *In re* Application for Tel. Info. Needed for a Criminal Investigation, 119 F. Supp. 3d 1011, 1024 (N.D. Cal. July 29, 2015) (describing surveys); Tracey v. State, 152 So. 3d 504, 526 (Fla. 2014), *reh'g denied* (Dec. 8, 2014) ("[A] subjective expectation of privacy of location as signaled by one's cell phone—even on public roads—is an expectation of privacy that society is now prepared to recognize as objectively reasonable . . . ." (citing Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring))). However, a few courts have allowed the government to obtain cell phone location information in real-time or prospectively without a warrant by combining multiple statutory justifications. *See, e.g.*, *In re* Application of the U.S. for an Order: (1) Authorizing the Installation & Use of a Pen Register & Trap & Trace Device; & (2) Authorizing Release of Subscriber Info. and/or Cell Site Info., 411 F. Supp. 2d 678, 680 (W.D. La. 2006); *In re* Application of the U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., 460 F. Supp. 2d 448, 450 (S.D.N.Y. 2006). And some have held that there is simply no expectation of privacy in cell location information. *See, e.g.*, United States v. Skinner, 690 F.3d 772, 781 (6th Cir. 2012), *cert. denied*, 133 S. Ct. 2851 (2013) (holding that when a device has built-in location-tracking function, there is no reasonable expectation of privacy in location data emitted by device, but also emphasizing that surveillance here lasted only three days); *In re* Application of the U.S. for an Order for Authorization to Obtain Location Data Concerning an AT&T Cellular Tel., 102 F. Supp. 3d 884, 889–90 (N.D. Miss. 2015) (holding that suspects did not have reasonable expectation of privacy in location data transmitted from cell phones); *In re* Smartphone Geolocation Data Application, 977 F. Supp. 2d 129, 147 (E.D.N.Y. 2013) (holding that users are well aware of the geolocation functions of their smartphones and have no reasonable expectation of privacy in the prospective location information they emit); Devega v. State, 689 S.E.2d 293, 300 (Ga. 2010) (holding, prior to *Jones*, that defendant had no expectation of privacy while on a public roadway, and use of "ping" information from his cell phone provider to locate his car and arrest him was merely a more sophisticated form of tracking approved in *Knotts*).

two courts have extended this reasoning to Stingrays, holding that they also require a warrant because of the significant privacy intrusion they enable and because they allow the police to locate people whom they would not have been able to find otherwise.[70] As one federal judge put it, "[a]bsent a search warrant, the [g]overnment may not turn a citizen's cellphone into a tracking device."[71]

Historical cell site location information (CSLI)[72]—that is, records of individuals' locations held by cell phone providers—has largely not garnered the same constitutional protection. In the main, courts view this data as governed by the third party records doctrine, which holds that there is no expectation of privacy in information that has been voluntarily shared with a third party—here, the cell phone provider.[73] This doctrine is losing force in the context of digital data, but it has not yet been authoritatively narrowed or overturned.[74]

3. Video Cameras

Video is a relatively old form of public surveillance, but it is continually being enhanced as the technology develops. Surveillance cameras can be outfitted or integrated with an array of additional technologies,[75] including

---

[70] State v. Andrews,134 A.3d 324, 327 (Md. Ct. Spec. App. 2016).

[71] United States v. Lambis, No. 15CR734, 2016 WL 3870940, at *3 (S.D.N.Y. July 12, 2016).

[72] *See, e.g.*, *In re* Application for Tel. Info. Needed for a Criminal Investigation, 119 F. Supp. 3d 1011, 1013–14 (N.D. Cal. 2015) (describing the process of gathering historical CSLI and the substance of the CSLI).

[73] *See* Smith v. Maryland, 442 U.S. 735, 744 (1979); United States v. Miller, 425 U.S. 435, 443 (1976). For cases holding that CSLI is not protected by the Fourth Amendment for this reason, see United States v. Lang, 78 F. Supp. 3d 830, 835–36 (N.D. Ill. 2015) (collecting cases). *But see* United States v. Cooper, No. 13-cr-00693-SI-1, 2015 WL 881578, at *8 (N.D. Cal. Mar. 2, 2015) (holding that the government must get a warrant before obtaining sixty days' worth of historical CSLI).

[74] *See* United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) ("[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."); Michael W. Price, *Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine*, 8 J. NAT'L SECURITY L. & POL'Y 247 (2016).

[75] *See* Diane Cardwell, *At Newark Airport, the Lights Are On, and They're Watching You*, N.Y. TIMES (Feb. 17, 2014), http://www.nytimes.com/2014/02/18/business/at-newark-airport-the-lights-are-on-and-theyre-watching-you.html (describing the types of surveillance and data-collection technologies being integrated with LED light fixtures at Newark Airport).

gunshot detection systems,[76] license plate readers,[77] thermal imaging,[78] and advanced analytic software that purports to be able to recognize suspicious activity or crimes in process.[79] Facial recognition technology is becoming increasingly sophisticated as well, and police departments are beginning to augment surveillance cameras with real-time facial scanning.[80] Video cameras are also being trained to hand off to each other, following an individual's trail from one camera to the next, even if he or she disappears in between.[81] Other systems are "joined up," meaning that camera views can be shared and human operators can follow individuals from camera to camera.[82]

Building on that technology, comprehensive "Domain Awareness" surveillance systems are gaining footholds in American cities, giving police the ability to track the movements of individual persons and vehicles from afar.[83] Even cities without such comprehensive surveillance may nevertheless have access to hundreds or thousands of surveillance cameras, in both public and private networks.[84] Some jurisdictions monitor their video feeds in real time,

---

[76] *See* NANCY G. LA VIGNE ET AL., URBAN INST., USING PUBLIC SURVEILLANCE SYSTEMS FOR CRIME CONTROL AND PREVENTION: A PRACTICAL GUIDE FOR LAW ENFORCEMENT AND THEIR MUNICIPAL PARTNERS 3–4, 25–27 (2011), http://www.urban.org/UploadedPDF/412402-Using-Public-Surveillance-Systems-for-Crime-Control-and-Prevention-A-Practical-Guide.pdf.

[77] *Id.* at 27–28.

[78] *See* Kim Zetter, *Boston Bombing Investigation Exposed Successes, Failures of Surveillance Tech*, WIRED (May 29, 2013, 3:51 PM), http://www.wired.com/2013/05/boston-marathon-investigation/.

[79] *See* LA VIGNE ET AL., *supra* note 76, at 29–30.

[80] *See* U.S. GEN. ACCOUNTABILITY OFFICE, GAO-03-748, VIDEO SURVEILLANCE: INFORMATION ON LAW ENFORCEMENT'S USE OF CLOSED-CIRCUIT TELEVISION TO MONITOR SELECTED FEDERAL PROPERTY IN WASHINGTON, D.C. 35–36 (2003) (noting that CCTV systems in Tampa, Florida, and Virginia Beach, Virginia, were equipped with facial recognition software); CLARE GARVIE, ALVARO BEDOYA & JONATHON FRANKLE, GEORGETOWN LAW CTR. ON PRIVACY & TECH., THE PERPETUAL LINEUP 2, 22–23 (2016), https://www.perpetuallineup.org/. *But see* Zetter, *supra* note 78 (noting that facial-recognition system failed to identify Boston Marathon bombing suspects because surveillance cameras did not take full-frontal images).

[81] Lee Dye, *Surveillance Systems Are Getting Smarter*, ABC NEWS (Nov. 30, 2014, 6:20 AM), http://abcnews.go.com/Technology/surveillance-systems-smarter/story?id=27242336&singlePage=true.

[82] U.S. GEN. ACCOUNTABILITY OFFICE, *supra* note 80, at 35–36.

[83] Somini Sengupta, *Privacy Fears Grow as Cities Increase Surveillance*, N.Y. TIMES (Oct. 13, 2013), http://www.nytimes.com/2013/10/14/technology/privacy-fears-as-surveillance-grows-in-cities.html (discussing surveillance systems used in Oakland); Zetter, *supra* note 78 (discussing surveillance systems used in New York City); *see also* Heather Kelly, *After Boston: The Pros and Cons of Surveillance Cameras*, CNN (Apr. 26, 2013, 7:03 PM), http://www.cnn.com/2013/04/26/tech/innovation/security-cameras-boston-bombings/ (observing that the NYPD "can track cars and people moving through 1.7 square miles in lower Manhattan"); Craig Timberg, *New Surveillance Technology Can Track Everyone in an Area for Several Hours at a Time*, WASH. POST (Feb. 5, 2014), http://www.washingtonpost.com/business/technology/new-surveillance-technology-can-track-everyone-in-an-area-for-several-hours-at-a-time/2014/02/05/82f1556e-876f-11e3-a5bd-844629433ba3_story.html.

[84] *A Closer Look at Surveillance Cameras Post-Boston*, CBSNEWS (May 2, 2013, 11:13 AM), http://www.cbsnews.com/news/a-closer-look-at-surveillance-cameras-post-boston/ (noting that the Los Angeles Police Department has "about 700" cameras); Terry Atlas & Greg Stohr, *Surveillance Cameras Sought by Cities*

while others save the recordings for later viewing as needed, and many models provide both capabilities.[85]

Evidence that surveillance cameras deter crime is mixed at best.[86] Some studies have found that cameras contribute to a reduction in property crime, particularly vehicle thefts, but their impact is difficult to assess reliably since they are often coupled with other crime prevention efforts.[87] Because surveillance in public areas typically has been deemed not to be a Fourth Amendment search in the first place,[88] however, law enforcement has generally not been required to justify the use of surveillance cameras. Instead, the judiciary has historically permitted police to watch public areas or "open fields" without a warrant.[89]

After Boston Bombs, BLOOMBERG (Apr. 29, 2013), http://www.bloomberg.com/news/print/2013-04-29/surveillance-cameras-sought-by-cities-after-boston-bombs.html ("Chicago authorities have access to about 10,000 public and private video surveillance cameras . . . ."); L. Gordon Crovitz, *In Praise of Surveillance Cameras*, WALL ST. J. (Apr. 21, 2013, 5:22 PM), http://www.wsj.com/articles/SB10001424127887323309604578434712417328162 ("The most recent estimate, from 2010, is that Boston and surrounding towns have some 150 police surveillance cameras, plus 400 in the subway."); LA VIGNE ET AL., URBAN INST., EVALUATING THE USE OF PUBLIC SURVEILLANCE CAMERAS FOR CRIME CONTROL AND PREVENTION 23 (2011) (noting that Baltimore's "public surveillance program" contains more than 500 cameras); Sam Ford, *D.C. Police Gain Access to Private Surveillance Cameras*, WJLA (Oct. 31, 2014), http://wjla.com/news/crime/d-c-police-gain-access-to-private-surveillance-cameras-108628 (discussing the partnership between the D.C. Police department and a private security company, resulting in an additional 300 cameras for the police department).

[85] *See, e.g.*, NOAM BIALE, ACLU, EXPERT FINDINGS ON SURVEILLANCE CAMERAS 5 (2008), https://www.aclu.org/files/images/asset_upload_file708_35775.pdf; JERRY RATCLIFFE, DEP'T OF JUSTICE, VIDEO SURVEILLANCE OF PUBLIC PLACES 4 (2006), https://cops.usdoj.gov/pdf/pop/e02061006.pdf.

[86] *See, e.g.*, U.S. GEN. ACCOUNTABILITY OFFICE, *supra* note 80, at 21 ("[D]emonstrating a direct cause and effect relationship between decreased crime and CCTV may not be easy to do."); Sarah J. McLean, Robert E. Worden & MoonSun Kim, *Here's Looking at You: An Evaluation of Public CCTV Cameras and Their Effects on Crime and Disorder*, 38 CRIM. JUST. REV. 303, 323–24 (2013) (discussing some measurable impacts of surveillance cameras in Schenectady, New York); Brandon C. Welsh & David P. Farrington, *Public Area CCTV and Crime Prevention: An Updated Systematic Review and Meta-Analysis*, 26 JUST. Q. 716, 736 (2009) (reporting research that demonstrates the effectiveness of surveillance cameras at reducing vehicle crimes in car parks); LA VIGNE ET AL., *supra* note 84, at 39–41, 79–82 (discussing that surveillance cameras contributed to crime prevention in some areas of Baltimore and Chicago, but did not reduce crime in Washington, D.C.).

[87] BIALE *supra* note 85, at 3–5 (finding, in preliminary studies, that surveillance cameras contributed, at most, to some reduction in property crime in several California cities); Welsh & Farrington, *supra* note 86, at 736 (finding that surveillance cameras were most effective in reducing crime in car parks and vehicle crime and had little to no effect on other types of crime or crimes in broader public areas, and that some success was likely a result of other factors as well, such as improved lighting and security guards); RATCLIFFE, *supra* note 85, at 19 (concluding that "CCTV is more effective at combating property offenses than violence or public order crime" and "CCTV appears to work best in small, well-defined areas (such as public car parks)").

[88] California v. Ciraolo, 476 U.S. 207, 213 (1986) (holding that the Fourth Amendment does not "preclude an officer's observations from a public vantage point where he has a right to be and which renders the activities clearly visible").

[89] *See, e.g.*, United States v. Vankesteren, 553 F.3d 286, 290 (4th Cir. 2009) (holding that a pole camera did not violate the Fourth Amendment because it "was not placed within or even near the curtilage of

The landscape may be beginning to change. One court recently held that surreptitiously mounting a surveillance camera on a public utility pole and using it to monitor a private yard for six weeks was "so different in its intrusiveness that it [did] not qualify as a plain-view observation."[90] Even using a video camera to monitor a public business was found to have violated the Fourth Amendment rights of the store employee who was the subject of its most sustained surveillance, where the observation was "prolonged" and occurred from a "non-public vantage point" (because it was surreptitiously mounted out of sight).[91] Nevertheless, there is little consensus so far.[92]

4. Drones

Drones are unmanned flying crafts that can be as small as an insect or as large as a 757 passenger jet.[93] Much like surveillance cameras, they can be outfitted with a host of technologies, including high-powered cameras, thermal imaging devices, license plate readers, laser radar, eavesdropping devices, see-through imaging, scent detection, signals interception, and direction finding capabilities; facial or other biometric recognition devices are likely not far behind.[94] Drones are lighter than airplanes, generally cheaper, and require less fuel and no pilot.

[defendant's] home" and only captured activity in "open fields"); Rodriguez v. United States, 878 F. Supp. 20, 24 (S.D.N.Y. 1995) (approving of covert video surveillance of activities on public street); State v. Augafa, 992 P.2d 723, 734 (Haw. Ct. App. 1999) (upholding warrantless video surveillance of defendant on public sidewalk using camera on a pole nearby); McCray v. State, 581 A.2d 45, 48 (Md. Ct. Spec. App. 1990) (permitting covert video of defendant crossing the street). *But see* State v. Costin, 720 A.2d 866, 870 (Vt. 1998) (objecting to the notion of "indiscriminately" aiming video surveillance "at public places [to] capture[] lawful activities of many citizens in the hope that it will deter crime or capture what crime might occur").

90 Order Granting Defendant's Motion to Suppress, United States v. Vargas, No. CR-13-6025-EFS, at 20 (E.D. Wash. Dec. 15, 2014).

91 State v. Thomas, 642 N.E.2d 240, 246 (Ind. Ct. App. 1994).

92 *See, e.g.*, United States v. Cuevas-Sanchez, 821 F.2d 248, 250–51 (5th Cir. 1987) (holding that using a pole camera to record activities in defendant's backyard for two months was a Fourth Amendment search, and observing that "indiscriminate video surveillance raises the specter of the Orwellian state"); Shafer v. City of Boulder, 896 F. Supp. 2d 915, 942 (D. Nev. 2012) (holding that covert, long-term videotaping of private citizen's backyard violates the Fourth Amendment). *But see* United States v. Houston, 813 F.3d 282, 288–90 (6th Cir. 2016), *reh'g en banc denied* (2016) (holding that surreptitious installation of pole camera and warrantless surveillance of defendant's trailer and private property for ten weeks did not violate Fourth Amendment).

93 RICHARD M. THOMPSON II, CONG. RESEARCH SERV., R42701, DRONES IN DOMESTIC SURVEILLANCE OPERATIONS: FOURTH AMENDMENT IMPLICATIONS AND LEGISLATIVE RESPONSES 2 (2013), http://www.fas.org/sgp/crs/natsec/R42701.pdf.

94 *Id.* at 3–4; JAY STANLEY & CATHERINE CRUMP, ACLU, PROTECTING PRIVACY FROM AERIAL SURVEILLANCE: RECOMMENDATIONS FOR GOVERNMENT USE OF DRONE AIRCRAFT 5–6 (2011) [hereinafter PROTECTING PRIVACY], https://www.aclu.org/files/assets/protectingprivacyfromaerialsurveillance.pdf; Timothy T. Takahashi, *Drones and Privacy*, 14 COLUM. SCI. & TECH. L. REV. 72, 87–90 (2012); Declan McCullagh, *DHS*

The Department of Justice (primarily the FBI), the Department of Homeland Security, and the Department of Defense have begun using drones in at least a limited capacity.[95] The Customs and Border Protection arm of the Department of Homeland Security also has the authority to use drones in support of various federal, state, and local law enforcement activities, though flights are currently required to take place at heights that would largely preclude the collection of license plate data or facial pictures.[96] In addition, some local police departments have won permission to test and operate drones, though others have had their proposals squelched after public outcry.[97]

The Supreme Court historically has been unconcerned about surveillance by airplanes; those have been in the context of a one-time flyover, however, conducted at heights above the standard altitude at which drones are permitted

Built Domestic Surveillance Tech into Predator Drones, CNET (Mar. 2, 2013, 11:30 AM), https://www.cnet.com/news/dhs-built-domestic-surveillance-tech-into-predator-drones/; Patrick Tucker, *The Marines Want Mini-Missiles That Hunt for Specific Radio Signals*, DEF. ONE (Oct. 27, 2016), http://www.defenseone.com/technology/2016/10/marines-want-mini-missiles-hunt-specific-radio-signals/132717/.

[95] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-12-981, UNMANNED AIRCRAFT SYSTEMS: MEASURING PROGRESS AND ADDRESSING POTENTIAL PRIVACY CONCERNS WOULD FACILITATE INTEGRATION INTO THE NATIONAL AIRSPACE SYSTEM 8–9 (2012); THOMPSON, *supra* note 93, at 3; OFFICE OF THE INSPECTOR GEN., INTERIM REPORT ON THE DEPARTMENT OF JUSTICE'S USE AND SUPPORT OF UNMANNED AIRCRAFT SYSTEMS (2013) [hereinafter INTERIM REPORT], http://www.justice.gov/oig/reports/2013/a1337.pdf; PROTECTING PRIVACY, *supra* note 94, at 6–8; Letter from Stephen D. Kelly, Assistant Dir., Office of Cong. Affairs, FBI, to Sen. Rand Paul 1 (July 29, 2013), http://www.paul.senate.gov/files/documents/072913FBIResponse.pdf.

[96] *See, e.g.*, Letter from Rebecca Gambler, Director, Homeland Security and Justice, U.S. Gov't Accountability Office to Senator Mary Landrieu et al., 6, 30 (Sept. 30, 2014), https://www.hsdl.org/?view&did=758102; Brittany M. Hughes, *GAO: DHS Flew Drones for 1,726 Hours Over Interior of U.S.*, CNS NEWS (Oct. 3, 2014, 3:45 PM), http://cnsnews.com/news/article/brittany-m-hughes/gao-dhs-flew-drones-1726-hours-over-interior-us; *see also* OFFICE OF INSPECTOR GEN., U.S. DEP'T OF HOMELAND SEC., OIG-15-17, U.S. CUSTOMS AND BORDER PROTECTION'S UNMANNED AIRCRAFT SYSTEM PROGRAM DOES NOT ACHIEVE INTENDED RESULTS OR RECOGNIZE ALL COSTS OF OPERATIONS (2014), https://www.oig.dhs.gov/assets/Mgmt/2015/OIG_15-17_Dec14.pdf.

[97] *See, e.g.*, Christine Clarridge, *Seattle Grounds Police Drone Program*, SEATTLE TIMES (Feb. 8, 2013, 8:52 AM), http://www.seattletimes.com/seattle-news/seattle-grounds-police-drone-program/; Cyrus Farivar, *County Sheriff Finally Gets the Drone He Wanted, Ignores Privacy Concerns*, ARS TECHNICA (Dec. 3, 2014, 7:50 PM), http://arstechnica.com/tech-policy/2014/12/county-sheriff-finally-gets-the-drone-he-wanted-ignores-privacy-concerns/; Susan Greene, *Colorado's Mesa County a National Leader in Domestic Drone Use*, COLO. INDEP. (June 6, 2013), http://www.coloradoindependent.com/127870/colorados-mesa-county-a-national-leader-in-domestic-drone-use; Jennifer Lynch, *Miami-Dade PD Releases Information About Its Drone Program; Will the FAA Follow Suit?*, ELEC. FRONTIER FOUND. (Apr. 13, 2012), https://www.eff.org/deeplinks/2012/04/miami-dade-pd-releases-information-about-its-drone-program-will-faa-follow-suit; James Pinkerton, *Use of Drones in Community Policing 'Uncharted Territory'*, HOUSTON CHRONICLE (Oct. 26, 2012, 8:37 AM), http://www.chron.com/news/houston-texas/houston/article/Use-of-drones-in-community-policing-uncharted-3981675.php; PROTECTING PRIVACY, *supra* note 94, at 7–8.

to operate and thus likely to pick out less detail.[98] While no court has yet had an opportunity to squarely consider law enforcement's use of drones, at least one court has noted that the airplane flyover cases "[might] have been decided differently if law enforcement's observations included more than a one-time naked-eye observation" of the area being monitored.[99] The court added, albeit in dicta, that "a drone's ability to constantly and covertly view and record an individual or setting infringes on the American public's reasonable expectation of privacy that they will not be constantly and covertly observed by the government without a warrant."[100]

5. License Plate Readers

License plate readers are also in increasingly wide use. Readers, which automatically capture the license plate numbers of passing cars, may be mounted on stationary poles, moving police cruisers, or handheld devices.[101] They can log the time and date, the vehicle's GPS coordinates, and pictures of the car; the newest technology also snaps pictures of the number of occupants inside.[102] Readers send the data to a software tool that compares all plates that pass by against a designated "hot list" (for instance, plates that are known to be stolen, or AMBER alerts).[103] Some also retain plate information for future use.

In addition to use by local and state law enforcement, the Department of Homeland Security and the Drug Enforcement Administration automatically log license plates at the border and in "hub cities and high-traffic corridors."[104] One

---

[98] Florida v. Riley, 488 U.S. 445, 447–50 (1989); California v. Ciraolo, 476 U.S. 207, 209, 214–15 (1986); *see also* FAA Modernization and Reform Act of 2012, Pub. L. No. 112-95, § 334, 126 Stat. 11, 76–77 (2012) (setting 400-foot limit for drone use); Dow Chem. Co. v. United States, 476 U.S. 227, 239 (1986).

[99] Order Granting Defendant's Motion to Suppress, United States v. Vargas, No. CR-13-6025-EFS, at 19 (E.D. Wash. Dec. 15, 2014).

[100] *Vargas*, No. CR-13-6025-EFS at 22; *see also* State v. Davis, 360 P.3d 1161, 1172 (N.M. 2015) (holding that "prolonged hovering [by a helicopter] close enough to the ground to cause interference with [the defendant's] property" was an unconstitutional violation of the subject's expectation of privacy).

[101] ACLU, YOU ARE BEING TRACKED: HOW LICENSE PLATE READERS ARE BEING USED TO RECORD AMERICANS' MOVEMENTS 4 (2013), https://www.aclu.org/feature/you-are-being-tracked.

[102] *See, e.g.*, Lily Hay Newman, *New Traffic-Enforcement Tech Peers into Your Car and Counts Passengers*, SLATE (Apr. 28, 2015, 3:26 PM), http://www.slate.com/blogs/future_tense/2015/04/28/automated_vehicle_occupancy_detection_looks_in_cars_counts_passengers_records.html; Dustin Slaughter, *Philly Police Admit They Disguised a Spy Truck as a Goggle Streetview Car*, MOTHERBOARD (May 12, 2016, 4:50 PM), https://motherboard.vice.com/read/philly-police-admit-they-disguised-a-spy-truck-as-a-google-streetview-car.

[103] *See, e.g.*, New York v. Davila, 901 N.Y.S.2d 787, 789 (N.Y. App. Div. 2010) (describing use of hot list); ACLU, *supra* note 101, at 5; INT'L ASS'N OF CHIEFS OF POLICE, PRIVACY IMPACT ASSESSMENT REPORT FOR THE UTILIZATION OF LICENSE PLATE READERS 2, 24–26 (2009), https://web.archive.org/web/20131024095529/http://www.theiacp.org/LinkClick.aspx?fileticket=N%2BE2wvY%2F1QU%3D&tabid=87.

[104] ACLU, *supra* note 101, at 27 & n.82.

arm of DHS, Immigration and Customs Enforcement, is also seeking to tap in to commercial license plate databases.[105] The data that is collected can be put in centralized databases and used to plot either the various locations of a particular vehicle or all of the vehicles at given locations.[106]

Reliable estimates suggest that there are tens of thousands of readers in operation across the United States,[107] some of which may be able to scan close to 2000 license plates per minute.[108] In some of America's biggest cities, the density and capacity of license plate readers allow for millions of license plate scans,[109] a vanishingly small number of which are actually connected to any crime or wrongdoing.[110] Some jurisdictions delete unneeded data immediately, while others keep the records for up to five years or even indefinitely.[111]

EZ-Pass readers are another mechanism to automatically log cars' travel. While they are typically used to speed a traveler's route through highway toll booths, their signal can be read by any transponder set up to register them.[112]

---

105 U.S. DEP'T OF HOMELAND SEC., DHS/ICE/PIA-039, PRIVACY IMPACT ASSESSMENT FOR THE ACQUISITION AND USE OF LICENSE PLATE READER DATA FROM A COMMERCIAL SERVICE (2015), https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-lpr-march2015.pdf; *see also* Julian Hattem, *Feds Scale Back Proposal for License Plate Tracking System*, THE HILL (May 4, 2015, 3:50 PM), http://thehill.com/policy/technology/240980-feds-scale-back-plan-for-license-plate-tracking-system (noting that the DHS plan was updated to start with only half the country, instead of whole country).

106 ACLU, *supra* note 101, at 5–6.

107 *See id.* at 7; Cyrus Farivar, *Your Car, Tracked: The Rapid Rise of License Plate Readers*, ARS TECHNICA (Sept. 27, 2012, 9:30 PM), http://arstechnica.com/tech-policy/2012/09/your-car-tracked-the-rapid-rise-of-license-plate-readers/.

108 Jennifer Lynch & Peter Bibring, *Automated License Plate Readers Threaten Our Privacy*, ELEC. FRONTIER FOUND. (May 6, 2013), https://www.eff.org/deeplinks/2013/05/alpr.

109 *See, e.g.*, Martin Austermuhle, *License to Track? D.C. Cameras Capturing Millions of License Plate Numbers*, WAMU 88.5 (Dec. 10, 2013), http://wamu.org/news/13/12/10/license_to_track_dc_police_cameras_capturing_millions_of_license_plate_numbers.

110 *See, e.g.*, ACLU, *supra* note 101, at 13–15; Austermuhle, *supra* note 109.

111 *See, e.g.*, BOS. POLICE, SPECIAL ORDER ON LICENSE PLATE RECOGNITION SYSTEM (2011), http://www.aclu.org/files/FilesPDFs/ALPR/massachusetts/4790-4793%20Boston_Special%20Order%2011_026.pdf (requiring deletion of data after ninety days); L.A. CTY. SHERIFF'S DEP'T, FIELD OPERATIONS DIRECTIVE ON AUTOMATED LICENSE PLATE RECOGNITION (ALPR) SYSTEM 4886 (2009), http://www.aclu.org/files/FilesPDFs/ALPR/missouri/alprpra_professionaldevelopmentandresearchbureau_kansascitymo_1.pdf (requiring deletion only after two years); OHIO EMERGENCY MGMT. AGENCY, FY 2010 REGIONAL PROGRAM GUIDANCE AND APPLICATION PACKAGE 14851 (2010), http://www.aclu.org/files/FilesPDFs/ALPR/ohio/14749-14851%20Department%20of%20Public%20Safety.pdf (requiring immediate deletion); MESQUITE POLICE DEP'T, ACLU OPEN RECORDS REQUEST FOR MPD ALPR RECORDS, 10465–66, http://www.aclu.org/files/FilesPDFs/ALPR/texas/alprpra_mesquitepd_mesquitetx%20(2).pdf (indefinite retention).

112 Mariko Hirose, *Newly Obtained Records Reveal Extensive Monitoring of E-ZPass Tags Throughout New York*, ACLU (Apr. 24, 2015, 1:00 PM), https://www.aclu.org/blog/free-future/newly-obtained-records-reveal-extensive-monitoring-e-zpass-tags-throughout-new-york.

New York City has installed machines at intersections throughout the city to scan all EZ-Pass readers, ostensibly to facilitate traffic management.[113]

These technologies have not encountered constitutional impediments: the Supreme Court has emphasized on multiple occasions that because of "the pervasive regulation of vehicles capable of traveling on the public highways," there is no expectation of privacy in the content of license plates.[114] In keeping with this doctrine, courts have regularly held that law enforcement officers may, at their discretion and without any reasonable suspicion, do at least an initial check of a license plate against a law enforcement database.[115]

This right is not absolute. Where an officer uses the database to acquire information that a person "reasonably expect[s] would be unavailable to the police" or whether the acquisition violates police guidelines, constitutional protections may come into play.[116] Law enforcement authority is also cabined by Fourteenth Amendment restrictions on engaging in a discriminatory pattern of stops.[117] Moreover, there are arguably heightened Fourth Amendment consequences when it comes to a network of license plate readers that keep records of cars' locations over time, information not readily available to the public. Unlike individual plate checks, the creation of a database of presumptively innocent people's movements is not closely tied to the regulatory purposes cited by the Supreme Court. The cases have not yet, however, grappled with this distinction.

---

113 *Id.*

114 California v. Carney, 471 U.S. 386, 392 (1985); *see also* New York v. Class, 475 U.S. 106, 113 (1986) ("[A]utomobiles are justifiably the subject of pervasive regulation by the State. Every operator of a motor vehicle must expect that the State, in enforcing its regulations, will intrude to some extent upon that operator's privacy . . . .").

115 *See, e.g.*, United States v. Diaz-Castaneda, 494 F.3d 1146, 1149 (9th Cir. 2007); United States v. Ellison, 462 F.3d 557, 563 (6th Cir. 2006); Olabisiomotosho v. City of Houston, 185 F.3d 521, 529 (5th Cir. 1999); United States v. Walraven, 892 F.2d 972, 974 (10th Cir. 1989); United States v. Matthews, 615 F.2d 1279, 1285 (10th Cir. 1980); Jones v. Town of Woodworth, 132 So. 3d 422, 425 (La. Ct. App. 2013); People v. Davila, 901 N.Y.S.2d 787, 791 (N.Y. App. Div. 2010); State v. Davis, 239 P.3d 1002, 1006 (Or. Ct. App. 2010); State v. Myrick, 659 A.2d 976, 979 (N.J. Super. Ct. Law Div. 1995).

116 *Diaz-Castaneda*, 494 F.3d at 1152; *see also* Delaware v. Prouse, 440 U.S. 648, 662 (1979) ("An individual operating or traveling in an automobile does not lose all reasonable expectation of privacy simply because the automobile and its use are subject to government regulation."); State v. Donis, 723 A.2d 35, 40 (N.J. 1998) (holding that law enforcement may not "random[ly] use" license plate databases "to secure 'the personal information' of motorists by police officers who had no reason to suspect wrongdoing").

117 *See, e.g.*, Whren v. United States, 517 U.S. 806, 813 (1996); Chavez v. Illinois State Police, 251 F.3d 612, 635, 648 (7th Cir. 2001).

6. Body-Worn Cameras

Police-worn body cameras are increasingly in vogue as well, particularly in the wake of high-profile shootings of civilians by law enforcement officers;[118] civil rights and civil liberties groups have advocated, albeit cautiously, for their use as a tool of police accountability and transparency.[119] The cameras are typically quite small and can be attached to an officer's sunglasses, lapel, or tie.[120] Some display a visual signature such as a red light when they are recording, while others maintain the same appearance whether they are recording or not.[121] Evidence from body cameras has led to the indictment of police officers for murder on at least two separate occasions.[122]

Courts have not yet tackled constitutional challenges to body cameras. Where body cameras only record discrete police-civilian interactions in public and are not used to track individuals over a longer period, a Fourth Amendment challenge would seem highly unlikely to be successful.[123] As with the other technologies, however, body cameras can be juiced up. A network of linked body cameras, for instance, programmed to run continuously, would offer a fairly comprehensive picture of day-to-day life on the street. If those cameras were equipped with facial or other biometric recognition technologies, any person captured in the background of an officer's daily travels could be tracked, particularly if the videos were paired with surveillance camera recordings. And a body camera deployed inside a home will capture information in a constitutionally protected area, raising additional Fourth Amendment concerns.

---

118 *See, e.g.*, Nicholas Quah & Laura E. Davis, *Here's a Timeline of Unarmed Black People Killed by Police over Past Year*, BUZZFEED (May 1, 2015, 4:46 PM), http://www.buzzfeed.com/nicholasquah/heres-a-timeline-of-unarmed-black-men-killed-by-police-over#.alX4KM33O.

119 *See, e.g.*, *Sens. Schatz, Paul & Reps. Brown, Ellison, Cummings Introduce Bipartisan Legislation to Help Expand Responsible Use of Police Body Cameras*, U.S. SENATOR FOR HAW. BRIAN SCHATZ (Mar. 26, 2015), http://www.schatz.senate.gov/press-releases/sens-schatz-paul-and-reps-brown-ellison-cummings-introduce-bipartisan-legislation-to-help-expand-responsible-use-of-police-body-cameras.

120 *See* Alexandra Mateescu, Alex Rosenblat & Danah Boyd, *Police Body-Worn Cameras* 5 (Data & Soc'y Research Inst., Working Paper, 2015), http://www.datasociety.net/pubs/dcr/PoliceBodyWornCameras.pdf.

121 *Id.* at 13.

122 Dana Ford, *University Cop Indicted for Murder in Shooting of Motorist Samuel DuBose*, CNN (July 30, 2015, 12:18 AM), http://www.cnn.com/2015/07/29/us/ohio-sam-dubose-tensing-indictment/; Haley Rush & Gabrielle Burkhart, *Officers to Stand Trial for Killing James Boyd*, KRQE NEWS (Aug. 18, 2015, 7:42 AM), http://krqe.com/2015/08/18/closing-arguments-set-in-albuquerque-police-shooting-case/.

123 *Cf.* United States v. Stile, No. 1:11-cr-00185-JAW, 2013 WL 6198179, at *3 (D. Me. Nov. 27, 2013) (rejecting a challenge to the constitutionality of dashboard cameras on the grounds that they simply capture a law enforcement interaction occurring in public).

7. Biometric Identification Technologies

Finally, most of the technologies described above can be enhanced with biometric recognition capabilities, which enable individual identification at a level far faster than manually poring through books of mug shots or databases of facial pictures. Biometric data can be collected via software that recognizes faces or other biometric indicators.[124] Existing databases already contain photographs, fingerprints, palm prints, iris scans, voiceprints, and DNA profiles, along with more basic information such as height, weight, eye and hair color, and identifying marks, scars, and tattoos.[125] Although successful facial recognition at present largely depends on a controlled environment, the technology is advancing rapidly.[126] Remarkably, fingerprints have been successfully recreated from photographs of people gesturing normally, and technology is being developed that scans and identifies a person's irises from up to thirty-six feet away, suggesting that a range of biometric data may soon be available without the subject's awareness.[127]

Courts have historically been relatively tolerant of law enforcement collection of biometric information—pictures, fingerprints, even blood samples, and more—and have rejected Fourth and Fifth Amendment challenges to these practices.[128] Nevertheless, while an in-depth analysis of the constitutionality of

---

[124] *Next Generation Identification (NGI)*, FBI, https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi (last visited Oct. 26, 2016).

[125] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-16-267, FACE RECOGNITION TECHNOLOGY: FBI SHOULD BETTER ENSURE PRIVACY AND ACCURACY (2016), http://www.gao.gov/assets/680/677098.pdf (indicating that as of 2015, sixteen states allow the FBI to search their photo databases—most including drivers' license photos and some including criminal mug shots—for facial recognition purposes, and that the FBI is currently pursuing contracts with eighteen other states to expand the repository of its Facial Analysis, Comparison, and Evaluation (FACE) Services Unit); Anthony Cuthbertson, *FBI Develops Tattoo Tracking Technology*, NEWSWEEK (June 3, 2016, 7:45 AM), http://www.newsweek.com/privacy-fbi-tattoo-surveillance-eff-466064; Jennifer Lynch, *New Report: FBI Can Access Hundreds of Millions of Face Recognition Photos*, ELEC. FRONTIER FOUND. (June 15, 2016), https://www.eff.org/deeplinks/2016/06/fbi-can-search-400-million-face-recognition-photos; *Next Generation Identification (NGI)*, *supra* note 124; s*ee also The Pros and Cons of Gathering Biometric Data*, NPR (Sept. 18, 2012, 1:00 PM), http://www.npr.org/2012/09/18/161355293/the-pros-and-cons-of-gathering-biometric-data (indicating that fingerprints are being collected as a result of minor traffic offenses).

[126] *See* Derrick Harris, *Google: Our New System for Recognizing Faces Is the Best One Yet*, FORTUNE (Mar. 17, 2015, 5:05 PM), fortune.com/2015/03/17/google-facenet-artificial-intelligence/.

[127] David Goldman, *Hackers Recreate Fingerprints Using Public Photos*, CNN MONEY (Dec. 30, 2014, 9:07 AM), http://money.cnn.com/2014/12/30/technology/security/fingerprint-hack/index.html; Robinson Meyer, *Long-Range Iris Scanning Is Here*, THE ATLANTIC (May 13, 2015), http://www.theatlantic.com/technology/archive/2015/05/long-range-iris-scanning-is-here/393065/.

[128] Refer to the following Fourth Amendment cases: Maryland v. King, 133 S. Ct. 1, 3 (2012) (DNA samples); Skinner v. Ry. Labor Execs' Ass'n, 489 U.S. 602, 606, 634 (1989) (blood testing); Cupp v. Murphy, 412 U.S. 291, 296 (1973) (fingernail scrapings); United States v. Dionisio, 410 U.S. 1, 15 (1973) (voice

these technologies and their intersection with public space surveillance is beyond the scope of this Article, biometric identification technologies raise unique issues, particularly since biometric data may be captured remotely from people not suspected of any wrongdoing and compared against extensive law enforcement databases and private troves of information.[129] In addition, unlike the other technologies canvassed here, biometric technologies enable a level of individualized identification that is unmatched. While a car or a phone may be presumptively associated with its owner, biometric identification technology tells us conclusively who is actually behind the wheel or holding the device.[130] This instant identification hastens a loss of the functional anonymity that effectively offers some privacy in public. When anyone can be identified from afar, at the push of a button, it will spell the end of the "practical obscurity,"[131] described in more detail below, that many people take for granted when they move about in public.

---

exemplar); United States v. Mara, 410 U.S. 19, 22 (1973) (handwriting exemplar); Davis v. Mississippi, 394 U.S. 721, 727 (1969) (fingerprints); Schmerber v. California, 384 U.S. 757, 771 (1966) (blood samples). Refer to the following Fifth Amendment cases: United States v. Hubbell, 530 U.S. 27, 35 (2000) (observing that criminal suspect "may be compelled . . . to provide a blood sample or handwriting exemplar" (footnotes omitted)); Wilson v. Collins, 517 F.3d 421, 431 (6th Cir. 2008) (DNA sample); United States v. Reynard, 473 F.3d 1008, 1021 (9th Cir. 2007) (blood samples and DNA profiles); United States v. Oriakhi, 57 F.3d 1290, 1299 (4th Cir. 1995) (voice sample).

[129] *See, e.g.*, *Dionisio*, 410 U.S. at 10 (upholding compulsion of voice exemplar in large part because the request came from a grand jury and was therefore accompanied by a variety of judicial oversight mechanisms, implying that the Fourth Amendment analysis could come out differently if voice or facial information were instead automatically captured without such controls, such as in the case of facial recognition technology deployed on a surveillance camera or other device); *In re* Grand Jury Proceedings (Appeal of Mills), 686 F.2d 135, 144–45 (3rd Cir. 1982) (Gibbons, J., concurring) (emphasizing the importance of structural restraints imposed by grand juries); Douglas A. Fretty, *Face-Recognition Surveillance: A Moment of Truth for Fourth Amendment Rights in Public Places*, 16 VA. J.L. & TECH. 430, 447 (2011) ("[B]y stepping in front of a face-identifying camera, a civilian is matched not only with his state-owned photograph but also any data associated with his name—residence, welfare status, employment, social security number, tax history, criminal record, child support compliance, etcetera."); Wayne A. Logan, *Policing Identity*, 92 B.U. L. REV. 1561, 1599 (2012) (observing that learning an individual's identity also provides law enforcement with "rapid access to criminal history or 'status' databases (for example, those listing alleged gang affiliations)"). For an in-depth treatment of the constitutionality of biometric identification technologies, see Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 MINN. L. REV. 407, 543 (2012).

[130] *See* Donohue, *supra* note 129, at 536–37 ("A GPS chip may reveal where the car goes, but the verification of personally identifiable information, which is at issue in remote biometric identification, is more invasive in its direct and personal link to a specific individual.").

[131] *See* U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 762 (1989) (balancing, in a FOIA case, the privacy interest in the "practical obscurity" of criminal rap sheets against the "public interest in their release").

II. A MULTI-FACTOR TEST FOR ANALYSIS OF SURVEILLANCE IN PUBLIC

Despite the wealth and range of new technologies available to law enforcement, the judiciary has not yet developed a single, coherent framework to address their Fourth Amendment repercussions. This Part teases out analytical strands from existing cases to construct a comprehensive approach to the constitutional ramifications of surveillance in public spaces. It proposes a multi-factor analysis that is sufficiently adaptable to apply to varied surveillance technologies, while offering a heightened level of structural rigor and a set of unifying themes. In addition, because the factors spring from current case law, this approach will allow courts to use familiar tools to approach new challenges with confidence, even before the Supreme Court weighs in on each new technology.

A. Why Isn't Katz *Alone Sufficient?*

A prefatory question: Why not simply retain the *Katz* test without more? Why isn't the time-tested inquiry into an individual's reasonable expectation of privacy sufficient? In fact, courts generally still use the *Katz* analysis to assess the constitutional implications of new technologies. This Article does not recommend fashioning a new approach out of whole cloth; the factors proposed here are, in essence, a more rigorous method of evaluating the reasonable expectation of privacy. At the same time, in an era of evolving technologies, the relative simplicity of *Katz* has become a liability, failing to incorporate a number of important constitutional questions. Any new approach, while building on the framework created by *Katz*, must account for those deficiencies.

To begin with, the *Katz* approach presumes, in Justice Alito's words, that the "hypothetical reasonable person has a well-developed and stable set of privacy expectations."[132] On the contrary, technology itself—its ubiquity and its convenience—can dynamically change those expectations. As people become more reliant on their devices, the technology may seem less intrusive, making the apparent privacy risks recede as well.[133] A test premised on the reasonable expectation of privacy must become more objective to account for that shift.

---

[132] United States v. Jones, 565 U.S. 400, 427 (2012) (Alito, J., concurring).

[133] *See In re* Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 121 (E.D.N.Y. 2011) ("Public ignorance [about the consequences of various technologies] cannot long be maintained.").

Moreover, the Supreme Court currently imposes more restrictions on technologies that are utilized primarily by law enforcement than those that are in wide use, an approach that puts constitutional rights on an unstable foundation. In *United States v. Kyllo*, for instance, the police used special heat-sensing technology to detect the possible presence of a marijuana-growing operation inside a private home.[134] The Court suppressed the introduction of the evidence on the grounds that using "sense-enhancing technology" to obtain information about the inside of a home that otherwise would have required a physical intrusion to acquire "constitutes a search," at least where the technology is "not in general public use."[135]

As invasive technologies become cheaper, however, it becomes increasingly likely that they will end up in the hands of both the public and law enforcement; a thermal imaging add-on, for instance, is now available for smartphones.[136] If the Supreme Court does not require a warrant for the police to use any technology to which the public has access, law enforcement's surveillance powers will inexorably expand, and they will do so based on technological advancements and the falling cost of technology, not on considered policy or constitutional analysis.[137]

In making constitutional rights dependent upon the shifting ground of personal expectations, the reasonable expectation of privacy test also makes the Fourth Amendment something of an outlier from other guarantees in the Bill of Rights. As scholar Marc Blitz has argued:

> The First Amendment protects the speech of someone even if he is ignorant of its protection and is resigned to being silenced; why should the Fourth Amendment not similarly protect someone's ability to avoid being videotaped from moment-to-moment even if he is, perhaps, mistakenly resigned to living in a world where such surveillance is permissible?[138]

---

134 533 U.S. 27, 29 (2001).

135 *Id.* at 34.

136 Megan Geuss, *FLIR One, Round Two: The Thermal Imaging Camera Drops $100, Gets a New Shape*, ARS TECHNICA (Aug. 21, 2015, 8:03 AM), http://arstechnica.com/gadgets/2015/08/flir-one-round-two-the-thermal-imaging-camera-drops-100-gets-a-new-shape/ (discussing how the public can now buy thermal imaging technology).

137 *Accord* Order Granting Defendant's Motion to Suppress, United States v. Vargas, No. CR-13-6025-EFS, at 27 (E.D. Wash. Dec. 15, 2014) ("Further, given the continued advancement of technology and reduction of cost in 'old technology,' the 'in general public use' doctrine may lose viability . . . .").

138 Marc Jonathan Blitz, *Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World That Tracks Image and Identity*, 82 TEX. L. REV. 1349, 1435–36 (2004).

It is anomalous, in other words, for our (possibly mistaken) understanding of our constitutional privacy rights to be dependent upon our knowledge about any given technology, rather than upon fundamental societal and historical commitments to privacy.

Katz's approach can also put the government in an enviable position: when a technology is first introduced, it is new, it is experimental, it is clumsy, and it is often rolled out secretly or in a limited trial, raising little communal ire. By the time the technology is in place and publicly revealed, and society has begun to grasp its true implications, it is too late; only an out-of-touch Luddite could be said not to understand, and implicitly consent to, all its potential uses. For the government, it is heads, we win; tails, you lose.

Finally, the *Katz* test's focus on individual privacy does not adequately take into account the harm that surveillance can do to other core interests protected by the Constitution, in particular the rights to speak and associate guaranteed by the First Amendment.[139] In the words of the U.S. Court of Appeals for the District of Columbia, "[t]he Supreme Court has repeatedly emphasized that one of the main reasons for adoption of the Fourth Amendment was to provide citizens with the privacy protection necessary for secure enjoyment of First Amendment liberties."[140] Justice Sotomayor echoed the risks posed to those values by surveillance in her concurrence in *United States v. Jones*:

> 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 [inexpensive location tracking]—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."[141]

---

[139] *Cf.* Bursey v. United States, 466 F.2d 1059, 1083 (9th Cir. 1972) ("When governmental activity collides with First Amendment rights, the Government has the burden of establishing that its interests are legitimate and compelling and that the incidental infringement upon First Amendment rights is no greater than is essential to vindicate its subordinating interests.").

[140] Reporters Comm. for Freedom of the Press v. AT&T Co., 593 F.2d 1030, 1054 (D.C. Cir. 1978), *cert. denied*, 99 S. Ct. 1431 (1979).

[141] 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)); *see also* United States v. Pineda-Moreno, 617 F.3d 1120, 1125 (9th Cir. 2010) (Kozinski, C.J., dissenting) ("The FBI need no longer deploy

These threats of abuse are not the product of fevered imaginations. The Virginia State Police, for example, recorded the license plate numbers of attendees at political rallies for Barack Obama and Sarah Palin, as well as President Obama's inauguration, and kept the data for over three years until ordered by the Attorney General to purge it.[142] Police in Denver, Colorado spied on anti-logging activists and, in response to a training on non-violence, shared license plate information with the FBI's Joint Terrorism Task Force.[143]

Cell phone tracking is susceptible to abuse as well. Michigan law enforcement officers were reported in 2010 to have asked a cellular provider for information about the cell phones that were gathering in the area of an anticipated labor union protest,[144] and Chicago police are alleged to have used Stingray technology to track participants in lawful protests.[145] One security expert has charged that cell phones used by Occupy Wall Street protesters were routinely logged by law enforcement as a way of tracking individuals involved in the movement.[146]

Moreover, surveillance technologies are frequently targeted at disfavored or marginalized populations, jeopardizing both First Amendment rights to freedom of religion and the Fourteenth Amendment's protections against discrimination. The New York City Police Department (NYPD), for instance, used license plate readers as part of its widespread surveillance of Muslim communities in the New York area and is alleged to have used surveillance cameras and a host of other surveillance techniques as well.[147] Similarly, an investigation of license plate

agents to infiltrate groups it considers subversive; it can figure out where the groups hold meetings and ask the phone company for a list of cell phones near those locations.").

142 Mark Bowes, *Police Recorded License Plates at Obama Inauguration*, RICHMOND TIMES-DISPATCH (Aug. 18, 2013, 12:00 AM), http://www.timesdispatch.com/news/local/crime/article_32678a59-f9e1-5e46-8336-d5f4ba076cb7.html.

143 Kristin Atkins, *Statement—Kirsten Atkins, Target of Illegal Spying*, ACLU, https://www.aclu.org/statement-kirsten-atkins-target-illegal-spying (last visited Oct. 27, 2016).

144 Michael Isikoff, *FBI Tracks Suspects' Cell Phones Without a Warrant*, NEWSWEEK (Feb. 18, 2010, 7:00 PM), http://www.newsweek.com/fbi-tracks-suspects-cell-phones-without-warrant-75099.

145 *Chicago Activists Claim Police Used 'Stingray' Surveillance During Garner Protests*, RT (Dec. 10, 2014, 2:45 AM), http://rt.com/usa/212915-protesters-chicago-police-stingray/.

146 Natasha Lennard, *Security Expert: All Occupiers' Phones Were Logged*, SALON (June 6, 2013, 3:00 PM), http://www.salon.com/2013/06/06/security_expert_all_occupiers_phones_were_logged/.

147 Adam Goldman & Matt Apuzzo, *NYPD Defends Tactics over Mosque Spying; Records Reveal New Details on Muslim Surveillance*, HUFFINGTON POST (Apr. 25, 2012), http://www.huffingtonpost.com/2012/02/24/nypd-defends-tactics-over_n_1298997.html; *see also* Hassan v. City of New York, 804 F.3d 277, 285–88 (3d Cir. 2015) (listing factual allegations by plaintiffs alleging extensive, targeted surveillance of Muslim community); DIALA SHAMAS & NERMEEN ARASTU, MAPPING MUSLIMS: NYPD SPYING AND ITS IMPACT ON AMERICAN MUSLIMS 14 (2013), http://www.law.cuny.edu/academics/clinics/immigration/clear/Mapping-Muslims.pdf.

readers in Oakland, California, found that they were located disproportionately in African-American and Latino neighborhoods, despite the fact that automobile crimes and offenses predominantly occurred elsewhere.[148]

This type of governmental surveillance has a measurable effect on people's behavior. For instance, many New York-area Muslim-Americans, rocked by revelations that the NYPD had been spying on them, reported that they stopped going to worship services or engaging in political discussions, and even became more cautious about calling the police to report crimes.[149] After Edward Snowden revealed the extent of the government's spying on Americans in June of 2013, one-third of American adults took at least one step to conceal their information, according to a Pew study.[150] Journalists and lawyers, who often work on particularly sensitive issues, felt the impact of the surveillance revelations especially keenly; many radically changed their practices, including using time-consuming encryption, traveling to speak with contacts in person instead of by phone, and even telling contacts that they could not guarantee confidentiality.[151]

For these reasons, the nebulous "reasonable expectation of privacy" framework that has grown out of *Katz* is increasingly inadequate for our modern age. This is not to say that courts should cease their investigation into whether there is an expectation of privacy that would cut against untrammeled law enforcement use of various surveillance technologies. Rather, the inquiry should be premised on relatively objective factors that take into account the full range of interests implicated by the Fourth Amendment, as set out below.[152] To be sure, a multi-factor test will not be entirely objective; judges can always overlay

---

148 Jeremy Gillula & Dave Maass, *What You Can Learn from Oakland's Raw ALPR Data*, ELEC. FRONTIER FOUND. (Jan. 21, 2015), https://www.eff.org/deeplinks/2015/01/what-we-learned-oakland-raw-alpr-data.

149 SHAMAS & ARASTU, *supra* note 147.

150 Lee Rainie & Mary Madden, *Americans' Privacy Strategies Post-Snowden*, PEW RESEARCH CTR. (Mar. 16, 2015), http://www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden/.

151 HUMAN RIGHTS WATCH, WITH LIBERTY TO MONITOR ALL: HOW LARGE-SCALE US SURVEILLANCE IS HARMING JOURNALISM, LAW, AND AMERICAN DEMOCRACY 4–5, 57 (2014), https://www.hrw.org/sites/default/files/reports/usnsa0714_ForUPload_0.pdf.

152 This approach would not replace existing constitutional protections for activities and items inside the home, which have a long pedigree, beginning with the clear text of the Fourth Amendment. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 37 (2001) ("The Fourth Amendment's protection of the home has never been tied to measurement of the quality or quantity of information obtained. In *Silverman*, for example, we made clear that any physical invasion of the structure of the home, 'by even a fraction of an inch,' was too much." (quoting Silverman v. United States, 365 U.S. 505, 512 (1961))). Instead, it would augment that core Fourth Amendment protection by providing a more rigorous structure for constitutional protection of certain activities outside the home.

their own preferences on top of each factor. But using these factors to build their analysis will prompt courts to grapple with the difficult issues they raise.

B. A Multi-Factor Approach to Public Space Surveillance

In light of the discussion above, this Article proposes six factors to guide the analysis of law enforcement's use of surveillance technologies to track people in public: (1) the length of time an individual is subject to surveillance; (2) the lowering of structural barriers to pervasive surveillance, as measured by reduction in cost and other resource allocations; (3) the creation of a recording that can be exploited to create a comprehensive picture of an individual's life or be mined for private, sensitive, or embarrassing moments; (4) the collection or receipt of information from inside a private home or other private space that would otherwise require a warrant; (5) erosion of core constitutional rights that traditionally have been understood to be protected by the Fourth Amendment; and (6) the combination of multiple surveillance technologies that may not trigger Fourth Amendment coverage standing alone, but pose significant risks to Fourth Amendment rights when taken together.

Enumerating these factors creates a framework that adds rigor to the constitutional inquiry, while retaining the flexibility that is a hallmark of Fourth Amendment analysis. Because these factors are technology-neutral, they can stand the test of time, rather than being left behind at the next set of innovations.

Other commentators, most notably David Gray and Danielle Citron, have advocated for an explicitly technology-dependent approach.[153] In their model, a technology would be subject to Fourth Amendment regulation if it could "facilitate broad and indiscriminate surveillance that intrudes upon reasonable expectations of quantitative privacy by raising the specter of a surveillance state" if "law enforcement officers or other government agents" were permitted to deploy and use the technology in their "unfettered discretion."[154] In other words, if a given technology *could* be used to facilitate a surveillance state by collecting a quantity of information that, *in toto*, intrudes on an individual's privacy, then *any* use of that technology would constitute a search.[155]

---

153 David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 73 (2013).
154 *Id.* at 71–72.
155 *See id.*

This is a thought-provoking and in some ways intuitively appealing model; it echoes the "theory of creepy" put forth by Omar Tene and Jules Polonetsky.[156] At the same time, I believe this model fails to grapple adequately with the practical ramifications arising from declaring that entire technologies trigger Fourth Amendment coverage, and I thus adopt a different approach.[157]

---

[156] Omar Tene & Jules Polonetsky, *A Theory of Creepy: Technology, Privacy, and Shifting Social Norms*, 16 YALE J.L. & TECH. 59, 60 (2013) (suggesting that "creepy" is increasingly being used as a "term of art" to "denote situations" in which our "social values" and our "technological capabilities" do not appear to align).

[157] In brief, while the technology-dependent proposal aligns with my concerns regarding the ability of modern-day technologies to enable a surveillance state, it leaves some important questions unanswered (or insufficiently answered). First, it neglects to account sufficiently for technologies that surely do not constitute a search on their first use but could be used to aggregate a constitutionally significant amount of data about a person; license plate readers come immediately to mind. Gray and Citron do acknowledge there will be close cases, but do not explain how to account for them, and close cases seem particularly difficult in an all-or-nothing model. *See* Gray & Citron, *supra* note 153, at 130 ("We therefore accept the inevitability of close cases. In doing so, however, we emphasize that the systemic burden of close cases will be much lighter under a technology-centered approach than they would be under a mosaic theory.").

The piece also seems to presume that a warrant would not always be required for searches, offering a variety of policy and statutory options. These alternatives may well be more nuanced and practicable than a warrant, and have much to recommend them. But constitutional doctrine requires that if the police carry out a search, they must obtain a warrant first (in the absence of a special need or another exception), and the proposal does not appear to sufficiently address how that process—which is key to the success of any Fourth Amendment regime, no small matter—would play out. *See, e.g.*, *id.* at 111 ("Applied to drones, GPS-enabled tracking, and similar technologies, this [warrant] requirement might mean setting limits on when, how, and how long a device can be deployed. A court might also require officers to take steps to minimize information about innocent third parties that is gathered incidentally. As in all Fourth Amendment cases, the guiding principle would be to strike a reasonable balance between the investigative needs of law enforcement and the privacy interests of the suspect and society at large."); *see also* Riley v. California, 134 S. Ct. 2473, 2482 (2014) (holding that where "a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing," the Fourth Amendment "generally requires the obtaining of a judicial warrant"); Katz v. United States, 389 U.S. 347, 357 (1967) (observing that "searches conducted outside the judicial process . . . are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions"). In particular, Gray and Citron's account of negotiated agreements like consent decrees is thought provoking, and may even prove to be efficient and privacy-protective, but it is not clear where those agreements fit into the warrant scheme. One is reminded of the Chief Justice's comment in *Riley v. California* that "the Founders did not fight a revolution to gain the right to government agency protocols." 134 S. Ct. 2473, 2491 (2014).

Even where the proposal implies that a warrant will be necessary, it is left unsaid exactly when it would come into play. For instance, the piece rightly raises constitutional alarms about New York City's Domain Awareness System, described here in Section I.B.3. *See* Gray & Citron, *supra* note 153, at 70 ("Granting law enforcement unfettered access to twenty-first century surveillance technologies like aerial drones, DAS [Domain Awareness System], and sweeping data collection efforts, implicates these same Fourth Amendment interests."). But if a warrant is to be obtained for the technology itself, at what point should that occur? When the first computer is purchased? When the first two machines are linked up? When license plate readers are added to the system? It is appealing to say that the technology itself should be covered, but when the technology is really a system of interconnected technologies, there's a bit of a boiling frog problem—at what point does the Domain Awareness System move from being a set of discrete items to the system itself? The authors also seem somewhat too optimistic about law enforcement's openness to tight regulations, since police departments have more frequently demonstrated obfuscation and overreach when it comes to surveillance technologies, as discussed

The analysis outlined here will necessarily be carried out "in the light of the values of freedom of expression," as the Supreme Court has directed.[158] In some circumstances, there may be standalone First Amendment claims either on top of or in place of Fourth Amendment claims, as described below.[159] Surveillance that targets or disproportionately affects protected groups may also give rise to Fourteenth Amendment claims, though that analysis is beyond the scope of this Article.

Courts will conduct a fact-sensitive inquiry in each case to determine which elements are triggered and how much weight to give to each. Courts already engage in a similar process to determine whether a particular law enforcement activity constitutes a search; indeed, the Supreme Court has observed that it has "consistently eschewed bright-line rules, instead emphasizing the fact-specific nature of the reasonableness inquiry."[160] This approach would provide guideposts for that inquiry. Courts do this in other contexts as well, including assessing fair use in the copyright arena[161] and evaluating the adequacy of a special needs search.[162] Thus, as one court concluded in requiring a particularized warrant for thirty days' worth of phone tracking, while it may be difficult in some circumstances to identify the moment at which "the aggregation of data showing movement in public spaces crosses the line and becomes a 'search' . . . [,] courts have confronted similar problems in the past" and managed to weigh the various interests at hand.[163]

---

above. *See, e.g.*, *id.* at 123 (suggesting that "there is good reason to think that law enforcement agencies will be receptive" to regulation of surveillance).

These criticisms are not meant to undermine the overall force of the argument; there are, as this article acknowledges, challenges to a holistic approach. Gray and Citron do a powerful job of setting out an approach that would provide certainty for law enforcement with respect to each technology, once there is an initial determination regarding whether the technology would facilitate a surveillance state. These critiques are simply meant to clarify why this article chooses a different route.

158 Roaden v. Kentucky, 413 U.S. 496, 504 (1973); *see also* New York v. P.J. Video, Inc., 475 U.S. 868, 873 (1986) (indicating that First Amendment-protected materials are entitled to heightened procedural protections against searches and seizures); Marcus v. Search Warrant of Property at 104 East Tenth Street, Kansas City, Missouri, 367 U.S. 717, 729 (1961) ("The Bill of Rights was fashioned against the background of knowledge that unrestricted power of search and seizure could also be an instrument for stifling liberty of expression."); ABA STANDARDS ON CRIMINAL JUSTICE: TECHNOLOGICALLY-ASSISTED PHYSICAL SURVEILLANCE standard 2-9.1 (3d ed. 1999), http://www.americanbar.org/publications/criminal_justice_section_archive/crimjust_standards_taps_blk.html (recommending that courts weigh impact of surveillance on First Amendment freedoms in assessing new technologies).

159 *See* Part II.D.

160 Ohio v. Robinette, 519 U.S. 33, 39 (1996).

161 *See* Barton Beebe, *An Empirical Study of U.S. Copyright Fair Use Opinions, 1978–2005*, 156 U. PA. L. REV. 549, 554–55 (2008) (reviewing case law and describing four primary factors in a fair use analysis).

162 *See, e.g.*, New Jersey v. T.L.O., 469 U.S. 325, 337 (1985) (endorsing a balancing framework).

163 United States v. White, 62 F. Supp. 3d 614, 623–24 (E.D. Mich. 2014).

Needless to say, this approach is vulnerable to (at least) one major objection: sliding scale approaches are in danger of becoming "more slide than scale," as Anthony Amsterdam famously observed in his critique of Fourth Amendment jurisprudence.[164] This critique, as well as the practical need to give police enough certainty that they can reliably determine in advance whether a warrant is necessary, has led some scholars to advocate for a legislative approach. Christopher Slobogin, for instance, has proposed a detailed statutory structure that would require an escalating set of procedures to authorize governmental monitoring.[165] Orin Kerr has written in favor of statutory regimes as well, arguing that they are better suited to provide strong privacy protections.[166]

While the optimal outcome may be to obtain both statutory and judicial change, a statutory approach alone will not suffice. As a practical matter, Congress is likely to pass a comprehensive federal privacy and surveillance statute at approximately the same time D.C. becomes the fifty-first state with full voting representation—that is to say, never.[167] State legislatures may make more progress, and one could argue that it is appropriate for the states, as Brandeisian laboratories of democracy, to implement different privacy regimes depending upon the needs and political power of their respective citizenry.[168]

---

[164] Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 394 (1974).

[165] Christopher Slobogin, *Making the Most of* United States v. Jones *in a Surveillance Society: A Statutory Implementation of Mosaic Theory*, 8 DUKE J. CONST. L. & PUB. POL'Y (SPECIAL ISSUE) 1, 4–5 (2012). In Slobogin's framework, surveillance of an individual lasting less than twenty minutes could be carried out without any process. *Id.* at 25. Surveillance of between twenty minutes and forty-eight hours in aggregate would require reasonable suspicion and a court order. *Id.* at 27. And anything over forty-eight hours would require probable cause and a court order. *Id.* By contrast, a "general public search"—for instance, setting up CCTV cameras for general public safety surveillance—would not require a warrant or other court order at all, but would require that the group being surveilled have had access to a transparent political process that led to the installation of the camera. *Id.* at 30–32.

[166] Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 859–60 (2004) ("When technologies are new and their impact remains uncertain, statutory rules governing law enforcement powers will tend to be more sophisticated, comprehensive, forward-thinking, and flexible than rules created by the judicial branch. . . . Because early adopters of new technologies tend to have disproportionate political influence, legislators often will be unusually sensitive to privacy threats raised by technological change.").

[167] *See, e.g.*, Matt Fuller, *Will This Be the Most Do-Nothing Year of a Staunchly Unproductive Congress?*, HUFFINGTON POST (Apr. 29, 2016, 2:01 PM), http://www.huffingtonpost.com/entry/congress-accomplishments-do-nothing_us_5723801ae4b01a5ebde56947 (describing Congress's internal dysfunction and inability to pass significant legislation); Rachel Kurzius, *GOP Draft Platform Not So Hot On D.C. Statehood*, DCIST (Jul. 12, 2016, 11:26 AM), http://dcist.com/2016/07/gop_draft_platform_not_so_hot_on_dc.php (describing the Republican Party's opposition to D.C. statehood).

[168] *See* New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting) ("[A] single courageous State may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country.").

But a patchwork quilt of state statutes granting varying degrees of privacy protection is not adequate when foundational Fourth Amendment rights are at stake. Such a system would leave a fraction—likely a large fraction—of citizens deprived of critical constitutional guarantees.

To be sure, state legislatures, city councils, and even police departments could put in place *more* stringent protections than the Fourth Amendment requires, and they could act to implement safeguards before the courts reach consensus, as the Department of Justice has already done in requiring a warrant for Stingrays.[169] But those may not replace fundamental Fourth Amendment protections.

More broadly, Kerr has suggested that courts should adopt a bright-line approach rather than a sliding-scale analysis, invoking *Katz* as the paradigm:

> If courts must broaden Fourth Amendment rules in response to new technologies, the better approach is to rule that certain steps are always searches. The model should be the Supreme Court's famous decision in *Katz v. United States*, not the concurring opinions in *Jones*.
>
> . . . .
>
> . . . Under *Katz*, bugging and wiretapping that had been beyond Fourth Amendment protection were brought inside that protection to account for the new world of telephone communications. Notably, the *Katz* Court did not say that short-term bugging was permitted but that long-term bugging became a search at some unspecified point. Instead, the Court followed the traditional sequential approach by holding that *all* bugging of a phone while it was in a person's private use triggered the Fourth Amendment. Application of the same method to the use of relatively new surveillance techniques such as GPS surveillance suggests that the Court should choose between two basic options [adhering to *Knotts*/*Karo* or overturning them in full].[170]

This example proves too much, however. The pay phone wiretap in *Katz* was a different animal from modern-day surveillance. In *Katz*, the phone was either bugged or it was not; the police were either listening in or they were not.[171] The difficulty with emerging public surveillance technologies is precisely that they

---

[169] *See* U.S. DEP'T OF JUSTICE, DEPARTMENT OF JUSTICE POLICY GUIDANCE: USE OF CELL-SITE SIMULATOR TECHNOLOGY (2015), https://www.justice.gov/opa/file/767321/download (imposing a warrant requirement for most situations in which the FBI and other DOJ components use a Stingray; the policy does not apply to state or local law enforcement).

[170] Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 315, 353 (2012).

[171] *See generally* Katz v. United States, 389 U.S. 347 (1967).

do not lend themselves to such a strict demarcation. Few people would argue that flipping on a surveillance camera in public for a moment constitutes a search,[172] but following an individual for a month with a network of linked cameras is likely to appear to most people to tread on their Fourth Amendment rights to privacy. Declaring that *every* use of surveillance technology in public is a search is not consistent with effective and practicable policing; at the same time, declaring that *no* surveillance technology used in public constitutes a search is at odds with both evolving expectations of privacy and existing jurisprudence.

It is also notable that this approach—declaring that certain types of surveillance are either always a search or never a search—would be likely to significantly increase the number of situations in which a warrant is required, including those where it is not possible to get one either because the particularity requirement could not be satisfied or because the police do not yet have enough information to demonstrate probable cause. It is not clear what is meant to happen in those circumstances.

With these cautions in mind, the approach this Article proposes fleshes out and formalizes a task that courts have already undertaken to some degree; clarifies and articulates each factor; and offers *ex ante* guidance and certainty to law enforcement, the judiciary, and the populace alike. Armed with these factors, courts and law enforcement can determine more reliably and consistently where privacy, technology, and pervasive surveillance intersect with the demands of the Fourth Amendment.

1. Duration

a. Long-Term Surveillance: A Threat to Privacy and the First Amendment

The first factor is the length of the surveillance: specifically, whether it is of a duration that is longer than one would expect the police to accomplish without transformative technology.[173] The hallmark of many of the surveillance technologies described above is that they collect information over a far longer

---

[172] *But see* Gray & Citron, *supra* note 153.

[173] *Cf.* United States v. Carpenter, 819 F.3d 880, 895–96 (6th Cir. 2016) (Stranch, J., concurring) (calling for "a new test to determine when a warrant may be necessary" in cases involving the "long-term, comprehensive tracking of an individual's location," in light of the "quantity of records or the length of time" that may be at stake).

period of time than would be feasible without the technology,[174] and the information, taken as a whole, reveals far more than any individual point in time. Standing alone, this is often maligned (for reasons explained below) as the mosaic theory, but it captures a critical fact that the U.S. Circuit Court for the District of Columbia has emphasized:

> Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation.[175]

In other words, the whole is truly more than the sum of its parts. This long-term surveillance works a substantial intrusion on individuals' privacy and diminishes the obscurity that many people take for granted in their day-to-day movements. Courts have returned to this idea again and again in assessing these technologies. For instance, one district court recently held that thirty days of surveillance "extend[ed] well beyond what any reasonable person might anticipate," implicating the defendant's "subjective expectation [of privacy] in his movements over time."[176]

---

174 *See supra* note 111 and accompanying text.

175 United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010), *aff'd in part sub nom.*, United States v. Jones, 565 U.S. 400 (2012); *see also* United States v. Jones, 565 U.S. 400 (2012); Klayman v. Obama, 957 F. Supp. 2d 1, 36 (D.D.C. 2013), *vacated and remanded*, 800 F.3d 559 (D.C. Cir. 2015) ("Records that once would have revealed a few scattered tiles of information about a person now reveal an entire mosaic—a vibrant and constantly updating picture of the person's life.").

176 United States v. White, 62 F. Supp. 3d 614, 621–23 (E.D. Mich. 2014); *see also Jones*, 565 U.S. at 430 (Alito, J., concurring) (reasoning that "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy"); United States v. Graham, 824 F.3d 421, 447 (4th Cir. 2016) (en banc) (Wynn, C.J., dissenting in part and concurring in the judgment) ("Quantity matters, too. And in my view, the sheer volume of data the government acquired here decides this case."); United States v. Nerber, 222 F.3d 597, 602 (9th Cir. 2000) (observing that individuals have "a legitimate expectation to be free from *constant* video surveillance" (emphasis added)); United States v. Cooper, 2015 WL 881578, at *8 (N.D. Cal. Mar. 2, 2015) (suppressing sixty days' worth of location data obtained without a warrant on the grounds that a person has a reasonable expectation of privacy in location data and Congress did not intend the Stored Communications Act to cover this data); Order Granting Defendant's Motion to Suppress, United States v. Vargas, No. CR-13-6025-EFS, at 25 (E.D. Wash. Dec. 15, 2014) (emphasizing the "*prolonged* nature of the video surveillance"); *In re* Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 119 (E.D.N.Y. 2011) (holding that 113 days of historical cell phone records, showing the user's location, "capture[] enough of the user's location information for a long enough time period . . . to depict a sufficiently detailed and intimate picture of his movements"); *In re* Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 535, 539-42 (D. Md. 2011) (finding that Fourth Amendment requires probable cause warrant to access thirty days' worth of movement data); David Gray & Danielle Keats Citron, *A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy*, 14 N.C. J.L. & TECH. 381, 415 (2013) ("The tapestries of our lives are by definition an aggregation of events and activities that, when assessed discretely, or even iteratively, may have little

This is not a new approach: some thirty years ago, a federal district court opined in *Alliance to End Repression v. City of Chicago* that "there should come a point when, in tenaciously tracking and piecing together the details of a person's life from multifarious sources, the resulting probe becomes so intrusive as to amount to an invasion of privacy even if the individual pieces of the probe are from public sources."[177] Similarly, the appeals court in *Maynard*, the decision below in the *Jones* GPS tracking case, pinpointed the distinction between tasking an officer on the street to watch someone's movements versus doing the job via digital age surveillance:

> It is one thing for a passerby to observe or even to follow someone during a single journey as he goes to the market or returns home from work. It is another thing entirely for that stranger to pick up the scent again the next day and the day after that, week in and week out, dogging his prey until he has identified all the places, people, amusements, and chores that make up that person's hitherto private routine.[178]

The addition of technology has thereby both raised the stakes and lowered the barriers to intensive, intrusive surveillance.

The collection of this wealth of information can also impinge on the subject's First Amendment rights to freedom of religion, freedom of speech and association, and more.[179] As the *Alliance to End Repression* court recognized several decades ago, law enforcement's maintenance of a "dossier"—the pre-digital version of the comprehensive sweep of information now available via surveillance technologies—that was "so extensive as to create an entire portrait of [the subject's] personal, family, financial, and political life" was a "violat[ion of] her first amendment rights."[180]

Justice Sotomayor amplified this concern in her concurrence in *Jones*, noting that location surveillance can "generate[] a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial,

---

significance. When assessed holistically, however, these events not only tell a detailed story of our activities and associations, they may reveal who we are at a fundamental level and therefore expose opportunities for manipulation and control.").

177 627 F. Supp. 1044, 1054 (N.D. Ill. 1985).

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

179 *See* U.S. CONST. amend. I.

180 *Alliance to End Repression*, 627 F. Supp. at 1047, 1056 (adding that assembling details about a person's life "can only serve to stifle the very sort of lawful, robust dissent that the first amendment, from its inception, was intended to protect").

political, professional, religious, and sexual associations."[181] The knowledge that the government has access to such a broad scope of detailed information can thus have a chilling effect, making people reluctant to engage in speech, association, or dissent for fear of having the dragnet turned on them.

b. How Long Is Too Long?

It is easy to object to surveillance that is "very long"—but how long is too long? The current case law suggests that somewhere between six hours[182] and two weeks[183] is the sweet spot; no court has yet set a bright line, and courts may be unlikely to reach a point of precision.[184] At the same time, law enforcement needs more guidance than "you'll know it when you see it," since at that point it may be too late and the evidence suppressed.[185] I propose that the length of time that would invoke the durational factor is a period that is longer than the police would be expected to engage in surveillance under ordinary circumstances, using tools that require some human involvement. While admittedly not precise, this standard offers a benchmark for measuring a period of surveillance that would not raise constitutional questions, as against a period that would require the involvement of a neutral magistrate.

Thus, if an officer equipped with binoculars, a radio, or a car could and would follow an individual for four, six, or eight hours, that same duration enabled by

---

[181] *Jones*, 565 U.S. at 415 (2012) (Sotomayor, J., concurring); *see also* People v. Weaver, 909 N.E.2d 1195, 1199 (N.Y. 2009) ("[T]echnology yields and records with breathtaking quality and quantity . . . a highly detailed profile, not simply of where we go, but by easy inference, of our associations . . . .").

[182] Commonwealth v. Estabrook, 38 N.E.3d 231 (Mass. 2015); *see also* United States v. Scott, 2015 WL 4644963, at *6 n.7, *8 n.9 (E.D. Mich. Aug. 5, 2015) (ruling that ninety minutes of historical cell data was too brief a window to raise constitutional concerns, while emphasizing that the data did not reveal "precise historical location" and that there may be a "reasonable expectation of privacy in records . . . that encompass a longer period of time").

[183] *Estabrook*, 38 N.E.3d at 234 (ruling that request for two weeks of historical cell site location information required a warrant, regardless of the amount planned for use at trial); *see also Jones*, 565 U.S. at 430 (Alito, J., concurring in the judgment) (suggesting that location surveillance would trigger the Fourth Amendment "before the 4-week mark").

[184] *See* Coolidge v. New Hampshire, 403 U.S. 443, 474–75 (1971) (noting "the unstartling proposition that when a line is drawn there is often not a great deal of difference between the situations closest to it on either side"); *cf.* Gray & Citron, *supra* note 176, at 425 (noting that courts can choose, and have chosen, simply to lay down a bright line).

[185] *See, e.g.*, Dunaway v. New York, 442 U.S. 200, 213–14 (1979) ("A single, familiar standard is essential to guide police officers, who have only limited time and expertise to reflect on and balance the social and individual interests involved in the specific circumstances they confront."); Gray & Citron, *supra* note 176, at 409 ("Among the most important burdens of any Fourth Amendment standard is that it must provide clear guidance to police officers and lower courts. Muddy and unpredictable tests are both unfair and ultimately fail to provide substantial protection.").

one of the technologies covered here would not contribute to a finding of a search. Where the duration of surveillance is longer than would be practicable without scene-changing technology, however, it would go on the "search" side of the column.[186]

To be clear, when we talk about the duration of monitoring, we are referring to the monitoring of a specific individual or group, not simply an open area in which any given person is likely to appear only for a short time. This is so for the simple reason that Fourth Amendment claims are brought by defendants, and there must be an identifiable defendant (be it an individual or a group) who is surveilled for a long enough period that it gives rise to a Fourth Amendment injury. Where a network of interconnected cameras enables the tracking of a single individual or group traveling across the area covered by the cameras, the durational factor will come into play; the network essentially acts as a single tool of surveillance with capabilities far above any individual camera.

To be sure, the mosaic theory, which is essentially the durational factor by another name, has been criticized by a range of commentators. Orin Kerr, perhaps the most prominent challenger, has lodged both practical and doctrinal objections to the mosaic theory, arguing that it is difficult to administer and that it is essentially a holistic inquiry, in tension with the traditional, "sequential" Fourth Amendment approach that requires that a search spring from a single, discrete police action.[187] Yale scholar Priscilla Smith argues that the mosaic theory is simultaneously too broad—it could, in theory, apply to the aggregated visual observations of a beat cop over time, which is at odds with any workable notion of policing—and too narrow—it would not cover single, time-limited episodes of highly intrusive surveillance, which could impinge on constitutional rights.[188] The Supreme Court of Florida recently took aim as well, describing the mosaic theory as too problematic to reliably implement.[189]

Nevertheless, the inquiry into the duration of surveillance captures the judiciary's growing discomfort with the accumulation of details about individuals' lives; details that are far more revealing in aggregate than anything

---

[186] Of course, there are circumstances in which law enforcement would conduct a month-long stakeout, even if it required significant personnel and financial resources. Nevertheless, even a physical stakeout is qualitatively different from long-term electronic surveillance, which observes everything, no matter how picayune, and records it for later review.

[187] Kerr, *supra* note 170, at 314–15.

[188] Priscilla J. Smith, *Much Ado About Mosaics: How Original Principles Apply to Evolving Technologies in* United States v. Jones, 14 N.C. J.L. & TECH. 557, 563 (2013).

[189] Tracey v. State, 152 So. 3d 504, 520 (Fla. 2014).

that could have been gathered by even the most dogged and sleepless police officer. Moreover, because the durational approach would be one factor among several, rather than carrying the whole weight of the inquiry as with the mosaic theory, a given method of surveillance need not rise or fall solely on the somewhat ineffable question of how long is too long. As the government uses these technologies with more regularity, and as the courts issue more rulings on their constitutional implications, law enforcement agencies will be put on notice that a surveillance technology that could observe an individual or identifiable group for more than a brief duration stands a substantial chance of being rejected on constitutional grounds in the absence of a warrant, enabling them to go to a magistrate judge for approval on the front end.

2. Cost

The second factor for courts to consider is whether the surveillance is so much less costly, in terms of officer time, dollar costs, or other metrics, that it substantially reduces or even removes the practical barriers to dragnet surveillance. One of the defining aspects of digital age technology is that it allows surveillance that used to be expensive and time-consuming to be carried out so easily that police often no longer have to weigh the value and intrusiveness of the surveillance against the resources required to carry it out.[190] As Justice Sotomayor put it, because technological surveillance "is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: 'limited police resources and community hostility.'"[191] Monitoring that would have occupied a team of law enforcement officers working in shifts, around the clock, has been supplanted by technologies that require little investment of time and yield a wealth of data.

From a law enforcement perspective, this reduction in cost and manpower is a feature, not a bug. And to be clear, the increasing availability of cutting-edge technology to law enforcement is not in itself a constitutional problem; no one would expect police to continue to operate via teletypes and punch-card

---

[190] *See, e.g.*, United States v. Jones, 565 U.S. 400, 429–30 (2012) (Alito, J., concurring in the judgment) ("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. Only an investigation of unusual importance could have justified such an expenditure of law enforcement resources. Devices like the one used in the present case, however, make long-term monitoring relatively easy and cheap.").

[191] *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring) (quoting Illinois v. Lidster, 540 U.S. 419, 426 (2004)).

machines. But as courts are increasingly recognizing, this diminution in cost actually has significant constitutional consequences for privacy, by diluting structural privacy and "enabling an extent of surveillance that in earlier times would have been prohibitively expensive."[192] As the Supreme Court of Florida put it, invoking James Madison:

> [T]he ease with which the government, armed with current and ever-expanding technology, can now monitor and track our cell phones, and thus ourselves, with minimal expenditure of funds and manpower, is just the type of "gradual and silent encroachment" into the very details of our lives that we as a society must be vigilant to prevent.[193]

Justice Alito also flagged the relative ease and cheapness of GPS surveillance when he suggested, in his concurrence in *Jones*, that longer-term monitoring would trigger constitutional scrutiny.[194] And in ruling that long-term GPS surveillance was unconstitutional, the appeals court in *Maynard* emphasized the near-zero cost of GPS monitoring as against the time and expense of human surveillance:

> Continuous human surveillance for a week would require all the time and expense of several police officers, while comparable photographic surveillance would require a net of video cameras so dense and so widespread as to catch a person's every movement, plus the manpower to piece the photographs together. . . . [P]rolonged GPS monitoring is not similarly constrained. On the contrary, the marginal cost of an additional day—or week, or month—of GPS monitoring is effectively zero. . . . For these practical reasons, and not by virtue of its sophistication or novelty, the advent of GPS technology has occasioned a heretofore unknown type of intrusion into an ordinarily and hitherto private enclave.[195]

---

[192] United States v. Garcia, 474 F.3d 994, 998 (7th Cir. 2007); *see also* United States v. Powell, 943 F. Supp. 2d 759, 780 (E.D. Mich. 2013) ("[T]he government can often detail DEA agents to follow suspects on highways for a few hours almost as easily as they can track a cell phone. But the same technology and grant of authority, without more care, can also permit the government to conduct near-limitless around-the-clock surveillance of a person's location, subject only to the limitation of where the suspect may not have taken a cell phone.").

[193] *Tracey*, 152 So. 3d at 522 (quoting Klayman v. Obama, 957, F. Supp. 2d 1, 42 & n.67 (D.D.C. 2013)).

[194] *See Jones*, 565 U.S. at 430 (Alito, J., concurring in the judgment) (reasoning that "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy").

[195] United States v. Maynard, 615 F.3d 544, 565 (D.C. Cir. 2010) (footnote omitted) (citations omitted); *see also* People v. Weaver, 909 N.E.2d 1195, 1199 (N.Y. 2009) ("GPS is not a mere enhancement of human sensory capacity, it facilitates a new technological perception of the world in which the situation of any object may be followed and exhaustively recorded over, in most cases, a practically unlimited period. The potential for a similar

In other words, while the technology may not have been expressly designed for mass surveillance, the fact that it costs pennies on the dollar as compared to previous tracking methods means that law enforcement can monitor an individual's movements, or many individuals' movements, at a scale that simply would have been impossible in earlier decades. This ease, while surely valuable to law enforcement, also eliminates the practical barriers to dragnet surveillance that once existed.

To be clear, the cost to be taken into account is the cost of the surveillance itself, not the up-front costs associated with purchasing the particular surveillance device. The cost of the device itself will be amortized over its life, which will vary depending on the type of device, the frequency of its use, and the regularity with which new technologies are developed and rolled out.[196] In addition, the cost of investing in a particular technology may drop over time. Finally, judges already appear to base their cost comparison on the cost of conducting the surveillance,[197] and it is that cost that is most relevant to the lowered barriers to structural privacy. Once a surveillance technology is purchased, whether it costs $100 or $1000 or $10,000, it is the price of carrying out the surveillance that alters and perhaps erases the structural incentive for police to collect only the information they believe is really necessary.

In conducting this analysis, courts may decide to quantify the precise difference that triggers Fourth Amendment coverage. For instance, privacy advocates and experts Kevin Bankston and Ashkan Soltani have proposed that if a "new tracking technique" is at least ten times "less expensive than the previous technique, the technique violates expectations of privacy and runs afoul of the Fourth Amendment."[198] Alternately, courts may employ a more flexible, case-by-case analysis, taking into account the cautions articulated above.

Either way, as Justice O'Connor said some twenty years ago, "[w]ith the benefits of more efficient law enforcement mechanisms comes the burden of

---

capture of information or 'seeing' by law enforcement would require, at a minimum, millions of additional police officers and cameras on every street lamp.").

196 *See also* Kevin S. Bankston & Ashkan Soltani, *Tiny Constables and the Cost of Surveillance: Making Cents Out of* United States v. Jones, 123 YALE L.J. ONLINE 335, 341 (2014) ("[O]ur calculations do not include fixed costs, such as the cost of equipment, as they are amortized over time and over a large number of cases.").

197 *See, e.g.*, United States v. Powell, 943 F. Supp. 2d 759, 780 (E.D. Mich. 2013) (comparing following suspects on highway with monitoring a suspect's location via cell phone); *Maynard*, 615 F.3d at 565 (comparing cost of human surveillance with cost of GPS monitoring); *Jones*, 565 U.S. at 429–30 (Alito, J., concurring in the judgment) (comparing cost of "traditional surveillance" with long-term GPS monitoring).

198 Bankston & Soltani, *supra* note 196, at 337.

corresponding constitutional responsibilities."[199] (Peter Parker's Uncle Ben put it even more pithily: "[W]ith great power comes great responsibility."[200]) In other words, as the cost in time and resources of surveillance ratchets down, the constitutional import ratchets up.

3. Recording

The third factor for courts to consider is whether the surveillance technology creates a recording for later review. The existence of a recording raises several concerns, each constitutionally significant in different ways.

First, recording is the chief method for developing a mosaic of a person's life. Far more so than watching in real time, creating a recording enables the extraction of a host of interconnected inferences about an individual's associations, proclivities, and more. Indeed, recording will often be the *only* way to create a mosaic, since the ability to construct a mosaic depends on the compilation of enough data points—more than human memory can hold—to yield the big picture.[201] Recording thus enables the construction of comprehensive picture of a person's life that otherwise would be out of reach to all but her closest intimates. This information can also be used as a cudgel to "stifle . . . lawful, robust dissent."[202]

Relatedly, the creation of a recording enables the overlay of other technologies that pose heightened risks to privacy. Sophisticated data-crunching algorithms that analyze and extract ever-deeper levels of sensitive information, for instance, rely on a database of information that is accumulated by recording or compiling individual events.[203] Recording also enables the after-the-fact

---

199 Arizona v. Evans, 514 U.S. 1, 17–18 (1995) (O'Connor, J., concurring).

200 *Spider-Man Quotes*, IMDB, http://www.imdb.com/title/tt0145487/quotes (last visited Mar. 18, 2016).

201 *See, e.g.*, Marc Jonathan Blitz, *The Fourth Amendment Future of Public Surveillance: Remote Recording and Other Searches in Public Space*, 63 AM. U. L. REV. 21, 56 (2013) ("Recording is also usually indispensable to creating the kind of detailed 'mosaic' of a person's life, which the D.C. Circuit found so concerning and identified as a basis for subjecting GPS surveillance to Fourth Amendment limits.").

202 Alliance to End Repression v. City of Chicago, 627 F. Supp. 1044, 1056 (N.D. Ill. 1985).

203 *See generally* Peter Moskowitz, *The Future of Policing Is Here, and It's Terrifying*, GQ (Nov. 9, 2015, 2:27 PM), http://www.gq.com/story/the-future-of-policing-is-here-and-its-terrifying ("Cops are using software programs that use algorithms to analyze surveillance, GPS coordinates, and crime data to pinpoint specific areas where, and specific people who, might at some point commit a crime."); Kaveh Waddell, *Half of American Adults Are in Police Facial-Recognition Databases*, THE ATLANTIC (Oct. 19, 2016), http://www.theatlantic.com/technology/archive/2016/10/half-of-american-adults-are-in-police-facial-recognition-databases/504560/ (noting that facial recognition algorithms can compare surveillance and video with databases of ID photos or mugshots).

application of biometric identification technologies to pierce, quickly and seamlessly, the relative anonymity of law-abiding citizens.

Finally, a recording may pick up single, highly sensitive moments in time that would otherwise be essentially anonymous. Justice Sotomayor highlighted this concern in her concurrence in *Jones*, noting that individual 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 more are "indisputably private" in themselves.[204]

Notably, the technology to extract individual, sensitive details from a database of videotape is already here. For instance, one surveillance company has developed technology that enables quick searches for individuals, vehicles, and more:

> Its software can identify objects by shape, size and color. It can read license plates and recognize cars. When it comes to people, it can detect their gender, approximate age, mood and other demographic information. Using multiple cameras, it can track their patterns and some behaviors. It automatically zooms in on any person's face and identifies them based on things like the distance between their eyes or the shape of their nose.
>
> All that information is stored in a database. Big clues that would take a traditional investigator untold hours of watching video to uncover can be found with a 15-second search query.[205]

Of course, any police officer (or citizen) who is simply standing on the street could view these moments-in-time as well—no newfangled device needed. No court has suggested, nor does this Article propose, that officers should be

---

[204] United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) (quoting People v. Weaver, 909 N.E.2d 1195, 1199 (N.Y. 2009)); *see also* State v. Estrella, 286 P.3d 150, 157 (Ariz. Ct. App. 2012) (Eckerstrom, J., dissenting) ("If told that a stranger had been, without our knowledge, electronically tracking our movements, few of us would deny feeling some invasion had occurred. I also suspect that most Americans would consider such non consensual tracking to be an intrusion regardless of whether the tracking had (1) occurred for thirty days or thirty minutes, (2) followed only their movements in hypothetical public view, or (3) coincidentally disclosed any especially private event in their lives."), *review denied* (Jan. 8, 2013), *cert. denied*, 133 S. Ct. 2803 (2013); Smith, *supra* note 188, at 580–81 ("The most common examples of the technology's intrusiveness involve the possibility that certain information will be obtained—information that is found on just one 'tile' in the mosaic and that can be gathered from just one trip." Further noting that the concurring justices in *Jones* "do not completely jump on the mosaic bandwagon because they share a broader concern that Government spying could lead to a world in which the government needs only to run a quick search through the database to find something—just one thing—you wish it had not seen").

[205] Kelly, *supra* note 83.

restricted from using basic tools of policing, including: maintaining a presence in public, watching for potentially suspicious activities (in the course of which they might witness any number of sensitive or innocuous events), and drawing on their knowledge of a particular neighborhood or community to make sense of what they see.

Nevertheless, anyone who steps outside takes the risk that they may be seen, whether by a police officer or civilian, whether to the grocery store, the abortion clinic, or the NRA meeting. What they do not expect is that each of those moments will be recorded and kept in perpetuity for later discovery and analysis by a probing law enforcement officer, either wholesale or piecemeal. Marc Blitz has argued the point in detail:

> With comprehensive video archives, authorities would . . . be able to randomly stop and closely scrutinize numerous people on public streets, doing so this time by pausing on a person's image, enhancing or magnifying detail, and electronically matching aspects of each person's appearance against biometric or other databases.
>
> . . . .
>
> Such evidence, of course, has always been there for neighbors or strangers to see (and perhaps to spy on), but modern video surveillance now makes it possible (and potentially quite simple) for government to locate, gather, and store it en masse. Where we might have previously expected most of these interactions to exist only in people's memory if anywhere at all (and to fade soon afterwards), video surveillance allows officials to create permanent records of them that might be accessed years after they occur.[206]

Moreover, the distinction between being watched by a neighbor and watched (always, and in detail) by a law enforcement officer is constitutionally significant. As the Supreme Court of Vermont recently observed, "the protections of the Fourth Amendment are built around the recognition that one's relationship with a detached third party will be different than with an investigating officer."[207] Accordingly, technologies that record and store data for law enforcement use necessitate extra scrutiny. Significantly, in analyzing

---

[206] Blitz, *supra* note 138, at 1356, 1408; *see also* LAWRENCE LESSIG, CODE VERSION 2.0, 203 (2006) (distinguishing between simply monitoring behavior and making it searchable, noting that "[d]igital technologies change this balance—radically"); Renée McDonald Hutchins, *Tied Up in* Knotts*? GPS Technology and the Fourth Amendment*, 55 UCLA L. REV. 409, 455 (2007) ("[C]itizens of this country largely expect the freedom to move about in relative anonymity without the government keeping an individualized, turn-by-turn itinerary of our comings and goings.").

[207] *In re* Search Warrant, 71 A.3d 1158, 1178–79 (Vt. 2012).

whether the government may withhold records requested under the Freedom of Information Act to protect the privacy of individuals named in the records, the Supreme Court has long recognized an interest in a "practical obscurity" that effectively conceals personal details from the average observer.[208] This obscurity is undermined by the recording of information that can then be searched at leisure for evidence of sensitive, embarrassing, or simply private moments. As the Court has explained, the fact that "information regarding personal matters . . . may be available to the public in *some* form" does not extinguish a person's "interest in controlling the dissemination of [the] information."[209] There is, in other words, a "vast difference" between information that could be found "after a diligent search" and information found after "a computerized summary located in a single clearinghouse."[210] This is similar to the difference between tasking a police officer with following a person's movements, inevitably resulting in gaps and judgments about what to collect or record, and setting a tireless electronic bloodhound to do the same job.[211]

Technology has historically played a key role in this process, since "the computer can accumulate and store information that would otherwise have surely been forgotten long before a person attains age 80."[212] Databases of information—while an inevitable and indispensable part of the modern American bureaucratic state—have long raised red flags when it comes to constitutionally-protected interests and the possibility of governmental abuse.[213]

Moreover, retaining such recordings just in case the information becomes relevant in the future has shades of the general warrants that the Founders despised, and is contrary to the Fourth Amendment's requirement of individualized suspicion. It also brings to the fore the First Amendment concerns described earlier, as those sensitive pieces of personal information can be

---

[208] *See* U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 762–63 (1989) (balancing, in a FOIA case, the privacy interest in the "practical obscurity" of criminal rap sheets against the "public interest in their release").

[209] U.S. Dep't of Def. v. Fed. Labor Relations Auth., 510 U.S. 487, 500 (1994) (emphasis added).

[210] *Reporters Comm. for Freedom of the Press*, 489 U.S. at 764.

[211] *See generally* Woodrow Hartzog & Frederic Stutzman, *The Case for Online Obscurity*, 101 CALIF. L. REV. 1, 48 (2013) (fleshing out and advocating for a legal notion of obscurity to protect privacy on the Internet).

[212] *Reporters Comm. for Freedom of the Press*, 489 U.S. at 771.

[213] *See, e.g.*, Herring v. United States, 555 U.S. 135, 155 (2009) (Ginsburg, J., dissenting) ("Inaccuracies in expansive, interconnected collections of electronic information raise grave concerns for individual liberty."); Whalen v. Roe, 429 U.S. 589, 607 (1977) (Brennan, J., concurring) ("The central storage and easy accessibility of computerized data vastly increase the potential for abuse of that information . . . .").

accessed, used, and abused by the government to target dissidents, investigate lawful activist groups, or blackmail people into becoming informants.

Again, this is not a baseless fear. In a scathing dissent to an en banc Ninth Circuit decision allowing law enforcement to conduct DNA profiling of federal offenders on probation, Judge Reinhardt warned of the:

> [D]angers inherent in allowing the government to collect and store information about its citizens in a centralized place. J. Edgar Hoover terrorized leaders of the civil rights movement by exploiting the information he collected in his files. Our government's surveillance and shameful harassment of suspected communists and alleged communist-sympathizers in the middle of the twentieth century depended largely on the centralization of information collected about countless numbers of non-communist members of our citizenry—often by means that violated the Fourth Amendment. The same was true of the Palmer Raids a few decades earlier and of our roundup of Japanese Americans and their placement in internment camps during World War Two.
>
> Even governments with benign intentions have proven unable to regulate or use wisely vast stores of information they collect regarding their citizens. The problem with allowing the government to collect and maintain private information about the intimate details of our lives is that the bureaucracy most often in charge of the information "is poorly regulated and susceptible to abuse."[214]

When surveillance technologies record while they watch, therefore, courts must be alert to the risk that those recordings offer both a ready-made mosaic and a virtual time machine, available for after-the-fact review and exploitation, and law enforcement must be alert to the risk that their surveillance poses to Fourth Amendment rights.

4. Intrusion into Private Areas

The fourth factor for courts and law enforcement to consider is whether the technology reveals information about the inside of a private home that otherwise would require a warrant or an invitation for law enforcement to enter. If so, that will generally be dispositive.

---

[214] United States v. Kincade, 379 F.3d 813, 843 (9th Cir. 2004) (en banc) (Reinhardt, J., dissenting) (citing Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083 (2002)).

Since the start of challenges to surveillance in public, the Supreme Court has been sensitive to the risk that tracking technologies deployed in the open may nevertheless reveal information about a person's presence in a home or another private area, space that is scrupulously protected by the warrant requirement of the Fourth Amendment. In *United States v. Karo*, for instance, the Supreme Court analyzed whether it was constitutional to plant, without a warrant, a beeper in a can of ether that was delivered to a drug suspect and then carried inside a private home.[215] In light of *United States v. Knotts*, the Court was bound to hold that using the beeper to track the suspect in public did not implicate any constitutionally recognized expectation of privacy.[216] When the can of ether entered the private home, however, the calculus changed; at that point, the presence of the beeper inside the home revealed information that police otherwise would have had to get a warrant to obtain: that the subject was inside the home as well.[217] Notably, this was true even though visual observation of Karo (which would not have required a warrant) *could* have shown that the can entered the house; nevertheless, because the beeper revealed *conclusively* that the can stayed in the house, "a fact that could not have been visually verified," a warrant was required.[218]

Similarly, in *Kyllo v. United States*, the Supreme Court struck down the warrantless use of a remote thermal imaging device used to detect the presence of marijuana grow lights.[219] The Court held that when the police use "sense-enhancing technology" to obtain "any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area,'" it is a search.[220]

This same solicitude regarding incidental disclosure of information about the inside of a home—for instance, who is there and when—has been highlighted in recent surveillance cases as well, especially with respect to cell phone surveillance. For instance, the Florida Supreme Court, observed that:

> [B]ecause cell phones are indispensable to so many people and are normally carried on one's person, cell phone tracking can easily invade the right to privacy in one's home or other private areas, a matter that

215 468 U.S 705, 707, 709–11 (1984).
216 *Id.* at 713–14.
217 *Id.* at 715.
218 *Id.*
219 533 U.S. 27, 40 (2001).
220 *Id.* at 34 (quoting Silverman v. United States, 365 U.S. 505, 512 (1961)).

> the government cannot always anticipate and one which, when it occurs, is clearly a Fourth Amendment violation.[221]

A state court recently echoed this concern, reasoning:

> [B]ecause the use of the cell site simulator in this case revealed the location of the phone and [the defendant] inside a residence, we are presented with the additional concern that an electronic device not in general public use has been used to obtain information about the contents of a home, not otherwise discernable without physical intrusion. Under the applicable precedent, this is undoubtedly an intrusion that rises to the level of a Fourth Amendment "search."[222]

Thus, when a particular mode of surveillance is likely to enable the government to glean information about a protected space, and when the police will not know in advance that such information will be revealed and thus cannot avoid it, the Fourth Amendment comes into play and a warrant will be required.

5. Erosion of Core Constitutional Rights

Regardless of how the factors above play out, there are certain activities and certain categories of information that the Fourth Amendment has historically protected. For instance, communications that a person seeks to keep private, either by excluding "the uninvited ear," as Charles Katz did,[223] or by placing a written communication into an envelope and sending it via the U.S. Postal Service.[224]

Historically, protecting these communications from intrusion by the government has been relatively straightforward: close the phone booth door or seal the envelope. When technology has advanced enough to allow for interception despite these measures, the courts have caught up and imposed restrictions on the warrantless use of the technologies to ensure continued protection for these historical rights. For instance, both the wiretap in *Katz*[225] and the earlier "spike mike" that could be inserted directly into a house's wall to listen in on conversations were new technologies at the time, which the Court ultimately required a warrant to use.[226]

---

221 Tracey v. State, 152 So. 3d 504, 524 (Fla. 2014), *reh'g denied* (2014).

222 State v. Andrews, 134 A.3d 324, 349 (2016) (citing *Kyllo*, 533 U.S. at 34–35).

223 Katz v. United States, 389 U.S. 347, 352 (1967).

224 *See, e.g.*, United States v. Jacobsen, 466 U.S. 109, 114 (1984); *Ex parte* Jackson, 96 U.S. 727, 733 (1877).

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

226 Silverman v. United States, 365 U.S. 505, 506–07 (1961).

To be sure, the surveillance technologies canvassed in this paper primarily reveal information about a person's location or his or her activities in public, not the content of communications. Inevitably, however, technologies employed in public will enable the extraction of other types of information in unexpected ways, including the content of communications and other data. Courts will thus need to remain attentive to ensure that rights traditionally safeguarded by the Fourth Amendment remain protected.[227]

In a recent study, for instance, a group of MIT researchers recreated a conversation by remotely videotaping the vibrations triggered by the speech of the speakers.[228] Using a camera planted behind a sound-proof window, the researchers captured minuscule vibrations on a potato chip bag and the leaves of a plant, and crunched the data to reproduce the speech that created those vibrations.[229] Although the researchers used a sophisticated, high-speed camera, they discovered that a much cheaper, consumer-grade camera would have produced similar information as well.[230] To take a less sci-fi example, an observer trained in lip reading or sign language could use a surveillance camera, particularly one equipped with a zoom feature or other enhanced capabilities, to make out the content of a conversation without being physically present.

To be sure, conversations in public cannot always be expected to be private; when we sit with a friend in a busy restaurant or on a street bench, we take the risk that those around us may hear our conversation (though the very noise and bustle of a public area can provide some practical obscurity as well). But when we sit to talk to someone in a deserted café or a quiet corner, or when we keep our voices hushed and our tone low, we expect that our conversation will be kept just among the speakers; unanticipated, covert police surveillance that upends that expectation may be constitutionally suspect.

---

227 *See, e.g.*, United States v. Davis, 785 F.3d 498, 524 (11th Cir. 2015) (Rosenbaum, J., concurring) ("[W]hen, historically, we have a more specific expectation of privacy in a particular type of information, the more specific privacy interest must govern the Fourth Amendment analysis . . . ."), *cert. denied*, 136 S. Ct. 479 (2015).

228 *See, e.g.*, Rachel Feltman, *MIT Researchers Can Listen to Your Conversation by Watching Your Potato Chip Bag*, WASH. POST (Aug. 4, 2014), https://www.washingtonpost.com/news/speaking-of-science/wp/2014/08/04/mit-researchers-can-listen-to-your-conversation-by-watching-your-potato-chip-bag/; Glenn McDonald, *Conversation Heard in Potato Chip Bag Vibrations*, SEEKER (Aug. 7, 2014, 11:37 AM), http://news.discovery.com/tech/gear-and-gadgets/conversation-heard-in-potato-chip-bag-vibrations-140807.htm.

229 *See supra* note 228.

230 *Id.*

Katz itself was premised on precisely this understanding. When Charles Katz went to the pay phone to call his bookie, he closed the doors of the phone booth.[231] Once he was standing alone in the booth, he was entitled to operate on the presumption that no one could hear him speak, or divine the content of his conversation from afar.[232] Because Katz had sought to "preserve" his conversation "as private," even though it was "in an area accessible to the public," it was "constitutionally protected" against intrusion.[233] *Katz*'s progeny recognize that if speakers take steps to preserve the privacy of their conversations in public, even with no phone booth to protect them, eavesdropping on those conversations by means of enhanced technology—including one of the technologies described here or one not yet envisioned—requires a warrant.[234]

Courts have repeatedly recognized that Fourth Amendment rights must keep pace with technology. In then-Chief Justice Burger's words, "the Framers . . . intended the Fourth Amendment to safeguard fundamental values which would far outlast the specific abuses which gave it birth."[235] More recently, as the Supreme Court reiterated in *United States v. Jones*, "we must 'assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'"[236]

Thus, in a sharply critical concurrence in a case regarding historical cell site records, Eleventh Circuit Judge Robin Rosenbaum explained that where surveillance undermines our ability to "engage in activities in which we have historically maintained protected privacy interests," that surveillance may violate the Fourth Amendment.[237] Otherwise, "with every new technology, we

---

231 Katz v. United States, 389 U.S. 347, 352 (1967).

232 *See id.*

233 *Katz*, 389 U.S. at 351–53.

234 *See, e.g.*, Kee v. City of Rowlett, 247 F.3d 206, 208–09, 211 (5th Cir. 2001) (analyzing whether mourners at a public gravesite, who challenged police's warrantless installation of a microphone in an urn, took affirmative steps to keep their conversations private even while in public); *id.* at 217 (noting that the possibility of a violation of privacy is "increased when technological enhancements such as wiretaps are used"); United States v. Mankani, 738 F.2d 538, 542 (2d Cir. 1984) ("[T]he Fourth Amendment protects conversations that cannot be heard except by means of artificial enhancement."); *cf.* State v. Duchow, 749 N.W.2d 913, 915 (Wis. 2008) (analyzing when a speaker has reasonable expectation of privacy so as to trigger protections of wiretap law against interception).

235 United States v. Chadwick, 433 U.S. 1, 9 (1977), *abrogated by* California v. Acevedo, 500 U.S. 565, 579 (1991).

236 565 U.S. 400, 420 (quoting Kyllo v. United States, 533 U.S. 27, 34 (2001)).

237 United States v. Davis, 785 F.3d 498, 525 (11th Cir. 2015) (Rosenbaum, J., concurring) *cert. denied*, 136 S. Ct. 479 (2015).

surrender more and more of our historically protected Fourth Amendment interests to unreasonable searches and seizures."[238]

Although Judge Rosenbaum was critiquing the third party doctrine, her caution applies equally well to the personal information that may now be revealed simply by virtue of being exposed in public:

> [E]xisting Supreme Court precedent may fairly be construed to suggest that where society has historically recognized a legitimate expectation of privacy, we must continue to do so for purposes of Fourth Amendment analysis, even if, in our modern world, we must now expose to [the public] information that we would have previously kept private, in order to continue to participate fully in society. If we do not, we will face the Hobson's choice of leaving our historically recognized Fourth Amendment rights at the door of the modern world or finding ourselves locked out from it. That the Constitution will not abide.[239]

Our expectation of privacy in our communications, for example, has not waned simply because e-mail, which generally must be shared with Internet service providers, has largely replaced handwritten missives.[240] Similarly, the Internet was unknown to the Founders, but libraries were not.[241] Privacy and First Amendment interests in anonymous reading remain the same regardless of location, whether "we research and read . . . online at home or in a coffee shop instead of in hard copies of books and periodicals in the stacks of the library."[242] So, too, should certain core constitutional interests be protected whether they occur within the privacy of the home, within the four walls of a phone booth, or out in public.[243] This factor is likely to come into play relatively infrequently, but where it does, it will be critical for courts to be attentive to the preservation of these constitutional rights.

---

238 *Id.* at 523–33.

239 *Id.* at 527.

240 *Id.* at 528–29.

241 *Id.* at 529.

242 *Id.*

243 *See, e.g.*, Andrew Hilts, Christopher Parsons & Jeffrey Knockel, *Every Step You Fake: A Comparative Analysis of Fitness Tracker Privacy and Security*, CITIZEN LAB (Feb. 2, 2016), https://citizenlab.org/2016/02/fitness-tracker-privacy-and-security/ (noting that the majority of fitness tracking devices studies "emit persistent unique identifiers" that permit tracking of their wearers even "when the device is not paired, and connected to, a mobile device").

6. Combined Technologies

Finally, courts (and police) will need to pay special attention when technologies are combined or multiplied. A license plate reader can be added to a surveillance camera;[244] cameras can be networked to allow for more granular tracking;[245] drones can host movement-detection sensors, infrared sensors, and GPS capabilities;[246] and more. Indeed, New York City's Lower Manhattan Security Initiative combines a range of surveillance capabilities:

> [It] monitors 4,000 security cameras and license plate readers south of Canal Street. The project uses feeds from both private and public security cameras, which are all monitored 24 hours a day by the NYPD. Using face and object-detection technology, the police can track cars and people moving through 1.7 square miles in lower Manhattan and even detect unattended packages.[247]

Similarly, the Fresno, California, Police Department recently launched a Real Time Crime Center that allows instant access to hundreds of police, school, and traffic cameras, along with license plate databases, a gunshot detection system, and social media monitoring.[248] Reports indicate that videos from police body cameras and private surveillance camera systems may soon be added to the mix.[249]

When technologies are layered on top of each other, the factors outlined above will continue to guide the analysis, but some may take on special resonance. Police-worn body cameras are unlikely to trigger Fourth Amendment

---

244 *See* LA VIGNE ET AL., *supra* note 84, at 3.

245 *See* U.S. GEN. ACCOUNTABILITY OFFICE, *supra* note 80, at 38.

246 *See, e.g.*, *Domestic Unmanned Aerial Vehicles (UAVs) and Drones*, ELEC. PRIVACY INFO. CTR., https://epic.org/privacy/drones/#tech (last visited Oct. 29, 2016) ("Drones may also carry infrared cameras, heat sensors, GPS, sensors that detect movement, and automated license plate readers"); Timberg, *supra* note 83 (noting that infrared sensors on drones can be used to track people at night).

247 Kelly, *supra* note 83; *see also* Tim Dees, *NYPD's New Surveillance System: Multifaceted Protection, or a Little Orwellian?*, POLICEONE.COM (Sept. 25, 2012), http://www.policeone.com/police-products/investigation/video-surveillance/articles/5993550-NYPDs-new-surveillance-system-Multifaceted-protection-or-a-little-Orwellian/; Rocco Parascandola & Tina Moore, *NYPD Unveils New $40 Million Super Computer System that Uses Data from Network of Cameras, License Plate Readers and Crime Reports*, DAILY NEWS (Aug. 8, 2012, 8:50 PM), http://www.nydailynews.com/new-york/nypd-unveils-new-40-million-super-computer-system-data-network-cameras-license-plate-readers-crime-reports-article-1.1132135.

248 *See* Justin Jouvenal, *The New Way Police Are Surveilling You: Calculating Your Threat 'Score'*, WASH. POST (Jan. 10, 2016), https://www.washingtonpost.com/local/public-safety/the-new-way-police-are-surveilling-you-calculating-your-threat-score/2016/01/10/e42bccac-8e15-11e5-baf4-bdf37355da0c_story.html; *see also* Rory Appleton, *Fresno Police Unveil State-of-the-Art Crime Tracking System*, FRESNO BEE (July 7, 2015, 7:00 AM), http://www.fresnobee.com/news/local/crime/article26671756.html.

249 Appleton, *supra* note 248.

coverage on their own, for instance, but when the resulting videos are knitted together, or biometric recognition technology is added, the juiced-up surveillance technology that results may implicate constitutionally-protected privacy interests.

* * *

An important question has been left unanswered: in this fact-dependent inquiry, what weight are courts to give to each factor? Is one factor, standing alone, enough to determine that law enforcement has engaged in a search? Must there be three or four factors? How are courts and law enforcement to be guided in this inquiry?

As a practical matter, given their interconnectedness, it is highly likely that where one factor comes into play, others will follow. For instance, the reduced cost of surveillance (the second factor) makes it possible to aggregate large quantities of information over a period of time and create a mosaic (the concern animating the first factor). Such an aggregation will often be exploitable only if a recording is created, as reflected in the third factor. Moreover, as described below, any technology that is *highly* likely to reveal information about a private area that would otherwise be available only with a warrant, particularly where law enforcement cannot guard in advance against receiving such information, should be used only with a warrant; that factor is, in effect, a trump card.

The most difficult cases may be those in which, for instance, the duration is a bit longer than those in which courts so far have concluded that a warrant is not required, but not so long as to obviously require probable cause. In those cases, the other factors will be of particular relevance to the court, and it is likely that the good-faith exception will come into play until the doctrine solidifies. Similarly, police will need to pay particular attention to the overall impact of their surveillance technologies in determining, before the fact, whether they are likely to implicate Fourth Amendment privacy interests.

First Amendment principles will also play a critical role in this analysis.[250] In Yale Kamisar's words: "What good is freedom of speech or freedom of

[250] *See, e.g.*, Osborn v. United States, 385 U.S. 323, 341 (1966) (Douglas, J., dissenting) ("Privacy, though not expressly mentioned in the Constitution, is essential to the exercise of other rights guaranteed by it."); Lopez v. United States, 373 U.S. 427, 469–70 (1963) (Brennan, J., dissenting) ("[W]e must bear in mind that historically the search and seizure power was used to suppress freedom of speech and of the press . . . ."); Marcus v. Search Warrants of Property at 104 East Tenth Street, Kansas City, Missouri, 367 U.S. 717, 724, 729 (1961) ("Historically the struggle for freedom of speech and press in England was bound up with the issue of the scope of the search and seizure power."); Reporters Comm. for Freedom of the Press v. AT&T Co., 593 F.2d 1030,

religion or any other freedom if law enforcement officers have unfettered power to violate a person's privacy and liberty when he sits in his home or drives his car or walks the streets?"[251] Of course, most Fourth Amendment cases will not themselves involve rights to free speech or freedom of association; because these cases turn on the treatment by law enforcement of a criminal defendant, it is more likely that the defendant will stand accused of robbing a bank or transporting narcotics than trying to organize comrades for political advocacy. But as Judge Learned Hand exhorted in *United States v. Kirschenblatt*, we must not "forget that what seems fair enough against a squalid huckster of bad liquor may take on a very different face, if used by a government determined to suppress political opposition under the guise of sedition."[252] Judges should thus take into account the potential impact of the surveillance on foundational First Amendment values in determining how to weigh the factors in closer cases.

C. What Process Is Necessary?

When a court weighs the factors articulated above and concludes that the Fourth Amendment comes into play, what happens next? Where a given use of surveillance rises to the level of a search, the appropriate process will normally be a warrant, the *sine qua non* of Fourth Amendment protections.[253] It has not always been obvious, however, how to meet the Fourth Amendment's particularity requirement in the context of public space surveillance. The section below proposes a framework by which surveillance in public could be carried out consistent with the Fourth Amendment, and suggests that when the particularity standard cannot be met, the surveillance must be narrowed or discontinued. It also argues that the "special needs" doctrine, while superficially appealing in the context of law enforcement actions to deter or detect crime and terrorism, is rarely germane when it comes to law enforcement surveillance.

1054 (D.C. Cir. 1978), *cert. denied*, 440 U.S. 949 (1979) ("The Supreme Court has repeatedly emphasized that one of the main reasons for adoption of the Fourth Amendment was to provide citizens with the privacy protection necessary for secure enjoyment of First Amendment liberties."); *see also* Thomas P. Crocker, *The Political Fourth Amendment*, 88 WASH. U. L. REV. 303, 353 (2010) ("[P]olitical liberty is realized in the company of others, most notably in the freedom to associate with others and to peaceably assemble. These are public activities, not activities that remain private and undisclosed to others.").

[251] Yale Kamisar, *The Fourth Amendment and Its Exclusionary Rule*, 15 THE CHAMPION, Sept./Oct. 1991, at 20, 21.

[252] 16 F.2d 202, 203 (2d Cir. 1926).

[253] *See* Maryland v. King, 133 S. Ct. 1958, 1969 (2013) ("To say that the Fourth Amendment applies here is the beginning point, not the end of the analysis.").

1. Warrants and Particularity

The promises of the Fourth Amendment are backstopped by the requirement that, in almost all cases, the police must obtain a warrant based on probable cause to carry out a search. As the Supreme Court held in *Katz*, "searches conducted outside the judicial process . . . are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions."[254] The Supreme Court has repeatedly reiterated the supremacy of the warrant as a bulwark against overreach, observing that "the warrant requirement is 'an important working part of our machinery of government,' not merely 'an inconvenience to be somehow "weighed" against the claims of police efficiency.'"[255]

Furthermore, the mere fact that a warrant might impose certain logistical hurdles does not abrogate its status as a Fourth Amendment baseline. As Justice White has said, it is "hardly a compelling argument" against a warrant requirement to say that it would "oblige the Government to obtain warrants in a large number of cases."[256] Thus, when the Fourth Amendment comes into play, the presumptive standard is that a warrant is necessary.

To be valid, a warrant must meet constitutional tailoring standards: the Fourth Amendment requires warrants to "particularly describ[e] the place to be searched, and the persons or things to be seized."[257] Searches that do not or cannot satisfy this limitation—searches that are not susceptible to being described in this way because they are so broad-based—are constitutionally intolerable even with a warrant, since the only warrant that could accurately describe their scope would approach the general warrants that the Founders loathed.[258]

---

254 Katz v. United States, 389 U.S. 347, 357 (1967); *see also* Riley v. California, 134 S. Ct. 2473, 2482 (2014) (holding that where "a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing," the Fourth Amendment "generally requires the obtaining of a judicial warrant").

255 *Riley*, 134 S. Ct. at 2493 (quoting Coolidge v. New Hampshire, 403 U.S. 443, 481 (1971)).

256 United States v. Karo, 468 U.S. 705, 718 (1984); *see also King*, 133 S. Ct. at 1989 (Scalia, J., dissenting) ("Solving unsolved crimes is a noble objective, but it occupies a lower place in the American pantheon of noble objectives than the protection of our people from suspicionless law-enforcement searches. The Fourth Amendment must prevail.").

257 U.S. CONST. amend. IV.

258 *See, e.g.*, *In re* Search Warrant, 71 A.3d 1158, 1183 (Vt. 2012) ("The purpose of the particularity requirement is to prevent general searches. By limiting the authorization to specific areas and specific things, the particularity requirement ensures that the search will be carefully tailored to its justifications and will not become a wide-ranging, exploratory search that the Fourth Amendment prohibits." (citations omitted)).

This is particularly true of the type of unfocused, long-term surveillance enabled by many of the technologies described here. As one court explained:

> If law enforcement anticipates that a suspect will commit a crime *some place* at some future date, does that mean that law enforcement has probable cause to track a suspect *every place* he goes? The answer must be "No," lest general warrants be revived and the Fourth Amendment's particularly requirement be eviscerated. . . .
>
> Thus, when a law enforcement officer is queried by a magistrate as to where he wants to electronically track a suspect's movements, "everywhere" seldom, if ever, will be an acceptable answer.[259]

What, then, would a warrant scheme look like in the context of tracking an individual in public? How can the particularity requirement of the Fourth Amendment be met when it is impossible to particularly describe the place to be searched because the place may be every place the target goes over the course of a month? And how can the particularity mandate be squared with a search that sweeps in large quantities of information about innocent persons, as with a Stingray?[260]

The case law and the rules governing criminal proceedings in federal courts, taken together, suggest that when public space surveillance does rise to the level of a search, and a warrant is thus required, the following limitations apply: the warrant should be designed to make the information collection as narrow as feasible; the search must be reasonably limited in time; the search may not be constitutionally permissible at all if it will, de facto, obtain vastly more information than is relevant and necessary; and additional back-end minimization procedures may be necessary (but cannot substitute for front-end controls).

One magistrate judge, for example, recently imposed both *ex ante* and *ex post* limitations on the government's use of a Stingray device to bring the surveillance into compliance with the Fourth Amendment.[261] In that case, the judge was particularly concerned about the "inevitable . . . . collection of

---

[259] United States v. White, 62 F. Supp. 3d 614, 627 (E.D. Mich. 2014).

[260] Orin S. Kerr has suggested that it may be impracticable to meet the particularity requirement in the context of surveillance in public. Kerr, *supra* note 170, at 339. As detailed in this section, I believe that objection is manageable; a warrant often can be made particular enough to satisfy the constitutional standards. Where it cannot, the answer is not that a warrant is not needed but that the surveillance must be narrowed.

[261] *In re* Application of the U.S. for an Order Relating to Tels. Used by Suppressed, No. 15 M 0021, 2015 WL 6871289, at *3 (N.D. Ill. Nov. 9, 2015).

innocent third parties' information" via Stingray.[262] When the government submitted an application for a warrant to use a Stingray, the court therefore required three steps to limit the collection, retention, and use of the information gathered.[263]

First, police officers had to "make reasonable efforts to minimize the capture of signals from cell phones used by people other than the target of the investigation."[264] For example, the signal of the Stingray had to be as narrowly targeted as possible. Perhaps more importantly, officers were prohibited from using a Stingray "when, because of the location and time, an inordinate number of innocent third parties' information will be collected"—for instance, while standing outside a sports arena during a big event.[265] Second, all extraneous data—everything besides information identifying the particular phone used by the target—had to be destroyed within forty-eight hours after it was captured, and could not be held for searching down the line.[266] Finally, there was a total ban on the use of information about third parties.[267]

Courts have applied similar restrictions to video surveillance, borrowing generally from the strict requirements for electronic wiretap orders authorized by Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[268] For instance, in *Cuevas-Sanchez*, a pole camera case,[269] the order authorizing the installation of the camera limited the surveillance to thirty days and required the police to "minimize observation of innocent conduct and to discontinue the surveillance when none of the suspected participants were on the premises."[270] The Seventh Circuit has also imported the strict Title III requirements into the video surveillance context, holding that a warrant for video surveillance must limit the surveillance to thirty days maximum (with renewals available upon

---

262 *Id.*

263 *Id.* at 3–4; *accord* State v. Andrews, 134 A.3d 324, 360 (2016) (emphasizing the importance of both *ex ante* and *ex post* restrictions on Stingray use, holding that "[t]o allow the government to collect real-time location information on an unknown number of private cell phones, without any geographic boundaries, without any reporting requirements or requirements that any unrelated data be deleted, and without a showing of probable cause that contraband or evidence of a particular crime will be found through the particular manner in which the search is conducted would certainly run afoul of the Fourth Amendment").

264 *In re Application of the U.S. for an Order Relating to Tels. Used by Suppressed*, 2015 WL 6871289, at *3.

265 *Id.*

266 *Id.* at 4.

267 *Id.*

268 Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2511(2), 2518(7) (2012).

269 *See supra* note 92.

270 United States v. Cuevas-Sanchez, 821 F.2d 248, 249–50 (5th Cir. 1987).

judicial approval) and "be conducted in such a way as to minimize the interception of communications not otherwise subject to interception."[271]

Judges have imposed similar restrictions on the collection of electronic information as well. For instance, in a case relating to the 2013 mass shooting at the Washington Navy Yard, Magistrate Judge John Facciola chastised the government for seeking from Facebook a wide swath of information not only about the shooter but also about third parties with whom he had communicated or intersected in some way.[272] In response to the government's broad demand, the court crafted an order outlining the categories of information that the government was permitted to seize and those it was not.[273] The court also imposed after-the-fact minimization procedures to ensure that the government ended up in possession of only the information that was relevant to its investigation.[274] In light of the government's attempt to obtain far more information than was germane to the investigation, Judge Facciola warned that in the future, he might take steps to narrow the initial search parameters much more substantially.[275]

Similarly, the Ninth Circuit sitting en banc blasted the government in *United States v. Comprehensive Drug Testing* for overreaching, manipulation, and misrepresentation in its investigation of baseball players suspected of taking steroids.[276] Federal authorities obtained a warrant to search the facilities of Comprehensive Drug Testing, Inc. for the records of ten players as to whom they had probable cause.[277] When the warrant was served, however, "the government seized and promptly reviewed the drug testing records for hundreds of players in Major League Baseball (and a great many other people)."[278]

Because the information was already in the government's hands, the en banc court focused on affirming the lower court's orders directing the government to destroy or return the data that was outside the scope of the warrant.[279] More

---

[271] United States v. Torres, 751 F.2d 875, 883–84 (7th Cir. 1984); *see also* United States v. Biasucci, 786 F.2d 504, 507–10, 512 (2d Cir. 1986) (applying the reasoning from *Torres* to a similar challenge against video surveillance).

[272] *In re* Search of Info. Associated with Facebook Account Identified by Username Aaron.Alexis that is Stored at Premises Controlled by Facebook, Inc., 21 F. Supp. 3d 1, 6–9 (D.D.C. 2013).

[273] *Id.* at 5–6.

[274] *Id.* at 9–11.

[275] *Id.* at 11.

[276] 621 F.3d 1162, 1167, 1172 (9th Cir. 2010) (en banc) (per curiam).

[277] *Id.* at 1166.

[278] *Id.*

[279] *See id.* at 1167.

generally, however, the court warned that law enforcement's need to examine many electronic records as part of its search for a smaller universe of relevant materials "creates a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant."[280]

In concurrence, Chief Judge Alex Kozinski set out a detailed set of minimization protocols to ensure that law enforcement agents reviewed only information strictly relevant to the investigation.[281] Following the guidance in *Comprehensive Drug Testing*, the Supreme Court of Vermont subsequently confirmed that front-end restrictions can be "acceptable mechanisms for ensuring the particularity of a search."[282]

The restrictions above are relevant when a method of surveillance will capture information about a large number of people who are not related to the purpose of the search, but what about when the surveillance technology will be focused on an individual person and will collect information about that one person over a long period of time?

As with the examples above, the surveillance must still be tailored to collect information that is related to the probable cause of a crime that underlies the warrant. Thus, in *United States v. White*, the DEA obtained a search warrant authorizing agents to track Jimmie White II, a suspected drug trafficker, continuously for thirty days using his cell phone.[283] After White challenged the evidence gleaned through the cell phone tracking, a federal district court in Michigan concluded both that White "had a subjective expectation [of privacy] in his movements over time" and that that expectation was one society would recognize as reasonable.[284] While acknowledging that it is difficult to identify the precise point at which surveillance crosses the line into a Fourth Amendment search, the court reasoned that surveillance for over four weeks—particularly for a "garden variety drug trafficking crime"—is a "breach of one's reasonable expectation of privacy."[285] In light of that expectation, the surveillance had to be

280 *Id.* at 1176.
281 *Id.* at 1180 (Kozinski, J., concurring).
282 *In re* Search Warrant, 71 A.3d 1158, 1170 (Vt. 2012).
283 United States v. White, 62 F. Supp. 3d 614, 619 (E.D. Mich. 2014).
284 *Id.* at 623.
285 *Id.* at 624.

underpinned by a warrant hewing to the particularity requirement of the Fourth Amendment.[286]

The court ruled that the warrant had failed to satisfy the particularity standard because it authorized tracking for an extended time period in both public and private places.[287] Had the DEA instead "present[ed] a more tailored application for a warrant," they could have "satisfied the particularity requirement."[288] "For instance, the agent could have . . . appli[ed] . . . to track White for a limited period based on credible information that White was planning to engage in a drug transaction with the confidential informant at a particular time and place."[289] He could have provided information about the particular suppliers White was traveling to meet, allowing surveillance along those routes (even including overnight stays).[290] Or he could have suggested that White "stored drugs in one location and sold them out of another," and needed to be tracked between the two locations.[291]

Finally, where public surveillance technologies fall into the category of "tracking devices," Rule 41 of the Federal Rules of Criminal Procedure imposes specific warrant requirements.[292] A tracking device is an "electronic . . . device which permits the tracking of the movement of a person or object"—for instance, the beeper used in *Knotts* and *Karo*.[293] Under Rule 41, a warrant for a tracking device must "identify the person or property to be tracked" and "specify a reasonable length of time that the device may be used," which cannot exceed forty-five days (though forty-five day extensions are possible).[294] The person being tracked must also be notified of the tracking within a certain period of time after the tracking ends—generally ten days.[295]

---

286 *Id.* at 627; *see also* United States v. Powell, 943 F. Supp. 2d 759, 778 (E.D. Mich. 2013) (detailing the probable cause standard to be met for real-time cell phone tracking, including demonstrating that the person's location (particularly in protected places) is actually relevant to the crime at issue, and showing that both the specific cell phone and the person to be tracked are relevant to the investigation).

287 *White*, 62 F. Supp. 3d at 628–29.

288 *Id.* at 628.

289 *Id.*; *see also id.* at 628–29 (holding that a warrant "allow[ing] the police to track White at all times, night and day, on public streets and in private places, and into areas traditionally protected by the Fourth Amendment" was "akin to the general warrants condemned by the Founders" and was "repugnant to the Fourth Amendment").

290 *Id.* at 628.

291 *Id.*

292 FED. R. CRIM. P. 41; *see also* 18 U.S.C. § 3117 (2012).

293 18 U.S.C. § 3117(b) ("As used in this section, the term 'tracking device' means an electronic or mechanical device which permits the tracking of the movement of a person or object.").

294 FED. R. CRIM. P. 41(e)(2)(C).

295 FED. R. CRIM. P. 41(f)(2)(C).

Police-attached GPS devices would certainly qualify as tracking devices.[296] While cell phones permit the tracking of individuals, federal courts are currently split on whether they should legally be categorized as tracking devices, since they have many functions and are carried voluntarily.[297] Some courts have also held that historical cell site location information counts as information from a tracking device, meaning a warrant based on probable cause would be required to obtain that information;[298] critically, the owner of the phone would also need to be notified of the request.[299]

Where a warrant is required for a tracking device, there is still an open question as to what satisfies the probable cause requirement.[300] Some courts have held that simply identifying the person and the phone number to be tracked is sufficient.[301] Others have identified the same concerns animating the warrant

---

296 18 U.S.C. § 3117 (defining mobile tracking devices).

297 *See* The Honorable Brian L. Owsley, *The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in Its Electronic Surveillance*, 16 U. PA. J. CONST. L. 1, 44–45 (2013) (arguing that requests for access to cell site location information "should be filed pursuant to Rule 41 of the Federal Rules of Criminal Procedure"). *Compare* United States v. Powell, 943 F. Supp. 2d 759, 777 (E.D. Mich. 2013) ("[A] cell phone is not a 'tracking device . . . .'"), *and In re* Smartphone Geolocation Data Application, 977 F. Supp. 2d 129, 150 (E.D.N.Y. 2013) (concluding that a cell phone is not a tracking device), *and In re* Applications of U.S. for Orders Pursuant to Title 18, U.S. Code Section 2703(d), 509 F. Supp. 2d 76, 81 (D. Mass. 2007) (same), *and In re* Application of the U.S. for an Order for Disclosure of Telecomm. Records & Authorizing the Use of a Pen Register & Trap & Trace, 405 F. Supp. 2d 435, 449 (S.D.N.Y. 2005) (same), *with* United States v. Turner, 781 F.3d 374, 385 (8th Cir. 2015) (assuming without deciding that the defendant's cell phone should be treated as a tracking device), *and In re* Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't, 620 F.3d 304, 312–13 (3d Cir. 2010) (suggesting that while historical cell site location information likely does not count as information from a tracking device, prospective or real-time cell site information might), *and In re* Order Authorizing Prospective & Continuous Release of Cell Site Location Records, 31 F. Supp. 3d 889, 899 (S.D. Tex. 2014) (concluding that "prospective, continuous, and contemporaneous cell site monitoring" "converts a smartphone into a tracking device"), *and* United States v. White, 62 F. Supp. 3d 614, 624 (E.D. Mich. 2014) (holding that "a cell phone emitting geolocation data" fits into the definition of "tracking device" under 18 U.S.C. § 3117(b)), *and In re* Application of U.S. for & Order: (1) Authorizing Use of a Pen Register & Trap & Trace Device; (2) Authorizing Release of Subscriber & Other Info.; (3) Authorizing Disclosure of Location-Based Servs., 727 F. Supp. 2d 571, 580 (W.D. Tex. 2010) ("The bottom line is that cell phones undoubtedly have become 'electronic . . . device[s] which permit[] the tracking of the movement of a person or object.' They *are* tracking devices." (quoting 18 U.S.C. § 3117 (2006))).

298 *See, e.g.*, *In re* Application of the U.S. for an Order Authorizing Use of a Pen Register with Caller Identification Device Cell Site Location Auth. on a Cellular Tel., 2009 WL 159187, at *3 (S.D.N.Y. Jan. 13, 2009) (concluding that cell site location information is information from a tracking device).

299 FED. R. CRIM. P. 41(f)(2)(C).

300 *See In re Application of U.S. for & Order: (1) Authorizing the Use of a Pen Register & Trap & Trace Device; (2) Authorizing Release of Subscriber & Other Info.; & (3) Authorizing Disclosure of Location-Based Servs.*, 727 F. Supp. 2d at 581 ("Applying Rule 41 to CSLI requests also raises the issue of what precisely is meant by the requirement of probable cause in this context.").

301 *See, e.g.*, United States v. Wilford, 961 F. Supp. 2d 740, 772–73 (D. Md. 2013) (approving of applications to "ping" phone in order to locate it because, among other things, applications identified the number

restrictions described above; one court held, for instance, that to obtain a warrant to track a cell phone, police must demonstrate that "tracking the phone will *lead* to evidence of a crime," not simply that the phone is related to a crime, or that "a person has a cell phone and is engaged in criminal conduct."[302] This will be an area of further doctrinal development.

One last note: while upfront tailoring will be necessary to keep surveillance warrants within the bounds of the Fourth Amendment,[303] after-the-fact minimization requirements may be appropriate as well. Thus, for instance, a police department might need to delete excess video or cell phone records.[304] Any such deletion would need to comply with the government's obligations under *Brady v. Maryland*.[305]

2. Exceptions to the Warrant Requirement

While the warrant is the presumptive Fourth Amendment standard, there are certain scenarios in which a warrant is not required even though a Fourth Amendment search has occurred. Even in those circumstances, however, "the touchstone of the Fourth Amendment is reasonableness"—that is, the search must still be "reasonable" to pass constitutional muster.[306]

---

of the targeted cell phone and its user, even though the showing of probable cause only linked the individual to criminal activity rather than linking the phone itself); State v. Tate, 849 N.W.2d 798, 810 (Wis. 2014) (approving an order authorizing use of a Stingray and ruling that identifying the electronic serial number associated with the defendant's cell phone "satisfie[d] the particularity requirement because that number permits a particularized collection of cell site information for only one cell phone").

302 *In re Application of U.S. for & Order: (1) Authorizing the Use of a Pen Register & Trap & Trace Device; (2) Authorizing Release of Subscriber & Other Info.; & (3) Authorizing Disclosure of Location-Based Servs.*, 727 F. Supp. 2d at 584.

303 *See, e.g.*, Klayman v. Obama, 142 F. Supp. 3d 172, 192, 198 (D.D.C. 2015) (enjoining the National Security Agency's bulk collection of telephone metadata (albeit only with respect to the individual plaintiffs), holding that the unfettered acquisition and retention of vast databases of information was unconstitutional even if the government imposed limitations on its ability to search the data in the future).

304 *See, e.g.*, Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976) ("[T]o the extent such papers were not within the scope of the warrants or were otherwise improperly seized, the State was correct in returning them voluntarily and the trial judge was correct in suppressing others."); *In re* Search Warrant, 71 A.3d 1158, 1185–86 (Vt. 2012) (approving both before-the-fact restrictions and after-the-fact minimization requirements imposed upon use of data extracted from electronic devices).

305 373 U.S. 83, 87 (1963)

306 Florida v. Jimeno, 500 U.S. 248, 250 (1991); *see also* Brigham City v. Stuart, 547 U.S. 398, 403 (2006) ("[T]he ultimate touchstone of the Fourth Amendment is 'reasonableness'. . . ."); United States v. Knights, 534 U.S. 112, 118–19 (2001); Ohio v. Robinette, 519 U.S. 33, 39 (1996); Soldal v. Cook Cty., 506 U.S. 56, 71 (1992) ("'[R]easonableness is still the ultimate standard' under the Fourth Amendment . . . .").

Two exceptions will most often be invoked to justify a warrantless search via surveillance in public: exigent circumstances and special needs. They are briefly described below, with closer attention to the special needs doctrine, which allows for warrantless searches carried out for non-law enforcement purposes.[307] This doctrine has become something of a catch-all justification for searches that are ostensibly for the purpose of deterring crime or terrorism.[308] This section ultimately concludes, however, that when surveillance in public space rises to the level of a search, it is almost always for a law enforcement purpose, and thus requires a warrant.

a. Exigent Circumstances Exception

The exception for exigent circumstances comes into play when taking the time to obtain a warrant would put an individual's life or safety at risk—for instance, where a police officer needs to ensure that a suspect has been disarmed, prevent evidence from being destroyed, or chase a fleeing suspect in "hot pursuit."[309] In these cases, the warrant requirement gives way.

This exception would remain in place when it comes to real-time use of cutting-edge surveillance technologies, which might be deployed quite effectively to find or track an individual in an emergency. For example, a surveillance camera that zooms in on and follows an individual suspected of fleeing a murder scene until an officer can apprehend him, or a drone pressed into use to locate a victim of kidnapping where there are credible risks of imminent harm, would not typically require a warrant. As described below, longer-term individual tracking would still generally require a warrant.[310]

b. Special Needs Doctrine

The special needs exception also permits law enforcement to warrantlessly undertake certain searches that might otherwise require a warrant. The search

---

[307] Delaware v. Prouse, 440 U.S. 648, 659 n.18 (1979).

[308] Ric Simmons, *Searching for Terrorists: Why Public Safety Is Not a Special Need*, 59 DUKE L.J. 846 (2010).

[309] *See, e.g.*, Chimel v. California, 395 U.S. 752, 762–63 (1969) (authorizing search of arrestee to search for weapons and prevent the destruction of evidence); Warden v. Hayden, 387 U.S. 294, 298–99 (1967) (hot pursuit).

[310] *See infra* Parts III.C, III.D.

must be for a non-law enforcement-related purpose; a search that simply vindicates a "general interest in crime control" does not satisfy a special need.[311]

Whether searches for public safety qualify as a special need is a particularly knotty question. As argued below, the types of generalized surveillance typically deployed for public safety purposes frequently will not rise to the level of a search under the test articulated here.[312] When they do, however, can they be saved by the special needs analysis? Courts and commentators diverge over whether public safety qualifies as a special need.[313] I argue that public space surveillance that does constitute a search is not fundamentally in service of public safety: there is little empirical evidence that these surveillance technologies contribute to public safety, and their primary utility is clearly for identifying and locating suspects, a paradigmatic law enforcement goal.

i. Background

The special needs doctrine grew out of the need to search residential apartments to root out hidden violations of housing safety laws. In *Camara v. Municipal Court*, the Supreme Court first endorsed "administrative searches" of private homes to vindicate public safety regulations that could not be satisfied in any other way.[314] As long as there were "reasonable legislative or administrative standards for conducting an area inspection" that were "satisfied with respect to a particular dwelling," then probable cause to issue a warrant presumptively existed.[315] Unlike with a criminal warrant, the inspector did not have to show specific knowledge about the particular house or apartment, but an *ex ante* warrant was nevertheless required.[316]

---

311 *Prouse*, 440 U.S. at 659 n.18; *see also* Maryland v. King, 133 S. Ct. 1958, 1981 (2013) (Scalia, J., dissenting) (emphasizing that special needs searches "must be justified, *always*, by concerns 'other than crime detection'" (citation omitted)); Bd. of Educ. of Indep. Sch. Dist. No. 92 of Pottawatomie Cty. v. Earls, 536 U.S. 822, 833 (2002) (noting, in approving drug testing of students involved in extracurricular activities, that "the test results are not turned over to any law enforcement authority"); Ferguson v. City of Charleston, 532 U.S. 67, 84 (2001) (striking down a hospital's program to require all pregnant women to undergo drug tests because the program was designed in close coordination with law enforcement and the hospital planned to provide all positive results to the police); City of Indianapolis v. Edmond, 531 U.S. 32, 41 (2000) ("We have never approved a checkpoint program whose primary purpose was to detect evidence of ordinary criminal wrongdoing. . . . [W]e would not credit the 'general interest in crime control' as justification for a regime of suspicionless stops.").

312 *See infra* Part II.C.2.b.ii.

313 *See, e.g.*, Simmons, *supra* note 308, at 886 (discussing issue and collecting citations on both sides).

314 387 U.S. 523, 534, 537 (1967).

315 *Id.* at 538.

316 *Id.*

Two decades later, Justice Blackmun explicitly articulated the special needs doctrine in a case analyzing the propriety of an assistant vice principal's warrantless search of a high school freshman's purse.[317] Because a warrant was "unsuited" to the school environment, the majority in *New Jersey v. T.L.O.* concluded that "the legality of a search of a student should depend simply on the reasonableness, under all the circumstances, of the search."[318] Justice Blackmun elaborated in a frequently cited concurrence, explaining:

> Only in those exceptional circumstances in which special needs, *beyond the normal need for law enforcement*, make the warrant and probable-cause requirement impracticable, is a court entitled to substitute its balancing of interests for that of the Framers.[319]

As the Court subsequently emphasized in *City of Indianapolis v. Edmond*, programs undertaken to "detect evidence of ordinary criminal wrongdoing," even where the "gravity of the threat" is high, cannot be justified as a special need.[320] Instead, the purpose must be something other than "crime detection."[321]

Notwithstanding this implicit limitation on the scope of the doctrine, the Supreme Court and lower courts have endorsed a range of special needs searches and seizures in the decades since *T.L.O.*: drug tests of student athletes[322] and railway employees,[323] searches of public employees' workplaces for evidence,[324] stops on public highways looking for evidence of drunk driving or illegal immigrants[325] (though not possession of illegal drugs),[326] searches of

---

317 New Jersey v. T.L.O., 469 U.S. 325, 351 (1985) (Blackmun, J., concurring in the judgment).

318 *Id.* at 340–41.

319 *Id.* at 351 (Blackmun, J., concurring in judgment) (emphasis added).

320 531 U.S. 32, 41–42 (2000); *see also* Ferguson v. City of Charleston, 532 U.S. 67, 83 (2001) (striking down program requiring pregnant women to be tested for drugs because "the immediate objective of the searches was to generate evidence *for law enforcement purposes*").

321 Chandler v. Miller, 520 U.S. 305, 314 (1997).

322 *See* Vernonia School District 47J v. Acton, 515 U.S. 646, 648, 664–65 (1995); *see also* Bd. of Educ. of Indep. Sch. Dist. No. 92 of Pottawatomie Cty. v. Earls, 536 U.S. 822, 825 (2002) (permitting drug testing of students involved in extracurricular activities).

323 Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 634 (1989) (permitting drug testing of railway employees involved in train accidents).

324 O'Connor v. Ortega, 480 U.S. 709, 726 (1987).

325 United States v. Martinez-Fuerte, 428 U.S. 543, 562 (1976) (permitting suspicionless stop to question occupants of car regarding immigration status).

326 *See, e.g.*, City of Indianapolis v. Edmond, 531 U.S. 32, 40, 48 (2000) (prohibiting suspicionless stops for drug possession); Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 447 (1990) (permitting suspicionless sobriety checkpoint).

travelers' bags in a subway system,[327] and more. As criminal law scholar Stephen Schulhofer has put it,

> "[A]dministrative" scrutiny of homes, offices, personal effects, and even peoples' bodies has proliferated to the point where many Americans encounter these searches regularly at work, in schools, at the airport, on the highways, or in trains and buses. The once obscure administrative search doctrine now matters enormously in our daily lives.[328]

ii. Detection and Deterrence of Crime and Terrorism Is Not a Special Need

The warrant exception for special needs has had particular force where the government has asserted an interest in preventing acts of terrorism and other crimes. But categorizing the detection and prevention of crime, including terrorism, as a special need calls for considerable skepticism. Anticipating possible criminal acts, attempting to prevent them, and investigating them when they occur are, as the Supreme Court noted in *Edmond*, paradigmatic law enforcement functions;[329] they are notably dissimilar from the regulatory enforcement scheme approved in *Camara*[330] or even the public secondary school search in *T.L.O.*[331] To call these objectives a "special need," beyond the normal need for law enforcement, would be to wring the phrase of meaning.

To be sure, some would argue that terrorism is not "ordinary criminal wrongdoing."[332] Even exceptionally grave criminal threats, however, do not thereby trigger a special needs analysis—as the *Edmond* Court made clear.[333] At bottom, terrorism is a criminal act or, more often, a set of interconnected criminal acts. And experts, including the 9/11 Commission, suggest that it is

---

327 MacWade v. Kelly, 460 F.3d 260, 263 (2d Cir. 2006) (upholding searches in New York City subway system for purpose of preventing terrorist attacks).

328 STEPHEN J. SCHULHOFER, MORE ESSENTIAL THAN EVER: THE FOURTH AMENDMENT IN THE TWENTY-FIRST CENTURY 95 (2012). Professor Schulhofer has also offered one mechanism for distinguishing between types of special needs cases, differentiating those that involve the government's regulation of essentially private behavior (for instance, driving on the road) from those that involve governmental employees or partners (for instance, public school students). Stephen J. Schulhofer, *On the Fourth Amendment Rights of the Law-Abiding Public*, 1989 SUP. CT. REV. 87, 118.

329 *See Edmund*, 531 U.S. at 43–44.

330 Camara v. Mun. Court of San Francisco, 387 U.S. 523, 535 (1967).

331 New Jersey v. T.L.O., 469 U.S. 325, 341 (1985).

332 *See Edmund*, 531 U.S. at 41–42.

333 *See id.* at 42.

those criminal acts that provide the most promising opportunity to disrupt a terrorist plot.[334]

Allowing warrantless searches via surveillance would also make terrorism the camel's nose under the tent.[335] The Eleventh Circuit has most clearly articulated the risks of justifying surveillance on the grounds of perceived risks from terrorism. In *Bourgeois v. Peters*, a Georgia city argued that "post September 11," municipalities needed to be able to employ a magnetometer, or metal detector, at large gatherings in the absence of individualized suspicion.[336] The court rejected this bid, observing:

> While the threat of terrorism is omnipresent, we cannot use it as the basis for restricting the scope of the Fourth Amendment's protections in any large gathering of people. In the absence of some reason to believe that international terrorists would target or infiltrate this protest, there is no basis for using September 11 as an excuse for searching the protestors.[337]

The court acknowledged that "both protestors and passersby [might] be safer if the City were permitted to engage in mass, warrantless, suspicionless searches."[338] Nevertheless, the panel concluded,

> [T]he Fourth Amendment embodies a value judgment by the Framers that prevents us from gradually trading ever-increasing amounts of freedom and privacy for additional security. It establishes searches

---

334 *See, e.g.*, MARY DEROSA, CTR. FOR STRATEGIC AND INT'L STUDIES, DATA MINING AND DATA ANALYSIS FOR COUNTERTERRORISM 12 (2004), http://csis.org/files/media/csis/pubs/040301_data_mining_report.pdf ("Detecting combinations of these low-level activities—such as illegal immigration, operating front businesses, money transfers, use of drop boxes and hotel addresses for commercial activities, and having multiple identities—could help predict terrorist plots."); SIOBHAN O'NEIL, CONG. RESEARCH SERV., RL34014, TERRORIST PRECURSOR CRIMES: ISSUES AND OPTIONS FOR CONGRESS 1 (2007), http://www.fas.org/sgp/crs/terror/RL34014.pdf ("In order to meet [their] needs, terrorists engage in a series of activities, some of which are legal, many of which are not, including various fraud schemes, petty crime, identity and immigration crimes, the counterfeit of goods, narcotics trade, and illegal weapons procurement, amongst others."); *see also* M. ELAINE NUGENT ET AL., AM. PROSECUTORS RESEARCH INST., LOCAL PROSECUTORS' RESPONSE TO TERRORISM (2005), https://www.ncjrs.gov/pdffiles1/nij/grants/211202.pdf; NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT 181–82, 192–93 (2004), http://www.9-11commission.gov/report/911Report.pdf. Similarly, the would-be Millennium bomber Ahmed Ressam and his collaborators "were reported to all be involved in a series of criminal activities, to include credit card fraud, pick pocketing, shoplifting, and stealing identity documents." O'NEIL, *supra*, at 20.

335 *See, e.g.*, United States v. U.S. Dist. Court for the E.D. of Mich. (*Keith*), 407 U.S. 297, 320 (1972) (prohibiting the government from engaging in warrantless surveillance of alleged domestic terrorists).

336 387 F.3d 1303, 1311 (11th Cir. 2004).

337 *Id.* at 1311.

338 *Id.* at 1311–12.

> based on evidence—rather than potentially effective, broad, prophylactic dragnets—as the constitutional norm.[339]

As the Third Circuit recently observed, "the same rigorous [constitutional] standards" must be applied "even where national security is at stake."[340]

Moreover, even if crime and terrorism detection and deterrence did qualify as non-law enforcement-related needs, surveillance in public space would be a poor mechanism for accomplishing that goal. Courts require a fit between the special need asserted and the means proposed to address it;[341] a broad and indefinite monitoring scheme that is not narrowly targeted to the articulated threat is unlikely to pass constitutional muster.[342]

In *Camara*, for instance, the Supreme Court observed that there was "unanimous agreement" that the "*only* effective way" to ensure compliance with housing codes was through in-person inspections.[343] By contrast, in striking down a program of highway stops for the purpose of checking motorists' license and registration, the Justices in *Delaware v. Prouse* emphasized that while the state had an important interest in ensuring that only authorized drivers were on the road, the spot checks were not a "sufficiently productive mechanism to justify the intrusion upon Fourth Amendment interests."[344] Similarly, the Court has noted that the suspicionless checkpoint programs it has approved were "designed primarily to serve purposes *closely related*" to the relevant problems, be they border security or roadway safety from drunk drivers.[345]

In the context of potential violence or terrorism, courts have also required a connection between the public safety threat and the method of addressing it. In *Stauber v. City of New York*, for instance, a New York district court rejected the New York City Police Department's plan to search all attendees' bags prior to

---

339 *Id.* at 1312.

340 Hassan v. City of New York, 804 F.3d 277, 306–07 (3d Cir. 2015) (urging that even where the animating goal of surveillance is to prevent an act of terrorism, history teaches that "we must be . . . vigilant in protecting constitutional rights").

341 Stauber v. City of New York, No. 03 Civ. 9162(RWS), 2004 WL 1593870, at *33 (S.D.N.Y. July 19, 2004).

342 *See, e.g.*, Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 660 (1995) ("Finally, we turn to consider the nature and immediacy of the governmental concern at issue here, and the efficacy of this means for meeting it."); Klayman v. Obama, 142 F. Supp. 3d 172, 193 (D.D.C. 2015) ("I must also evaluate the efficacy of the searches at issue in meeting this need.").

343 Camara v. Mun. Court of San Francisco, 387 U.S. 523, 535–36 (1967) (emphasis added).

344 440 U.S. 648, 659 (1979).

345 City of Indianapolis v. Edmond, 531 U.S. 32, 41 (2000) (emphasis added).

demonstrations opposing the 2004 Republican National Convention.[346] The city argued that there could be an "increased risk of violence or of threats to public safety" if the NYPD was not allowed to conduct a dragnet bag search, citing to the fact that the federal government believed the Convention could be a target of terrorist attacks.[347] Rebuffing that argument, the court observed that the city had offered only a "general invocation of terrorist threats," with no showing of how the searches would mitigate the threat.[348]

To be sure, courts have approved suspicionless searches for the ostensible purpose of terrorism or threat mitigation. Even in those circumstances, however, they have emphasized the limits on the searches, indicating that a broad program of suspicionless surveillance would not pass muster.[349]

Critically, when it comes to surveillance in public space, there is little compelling evidence that surveillance actually succeeds in deterring most crime.[350] This thin record of efficacy suggests that the true function of many surveillance technologies will be to collect *evidence* of criminal activity for use during an investigation or prosecution—certainly a law enforcement purpose. As the *Bourgeois* court observed, while this would assuredly be useful, that is not the same as being constitutional.[351]

These and other special needs cases thus counsel strongly against permitting warrantless, broad-scale surveillance in the name of crime and terrorism detection and prevention. Importantly, this does not mean that cities can never use surveillance in support of public safety; as described below,[352] there are

---

346 2004 WL 1593870, at *33.

347 *Id.* at *31.

348 *Id.*; *see also* Commonwealth v. Carkhuff, 804 N.E.2d 317, 322–23 (Mass. 2004) (ruling that stops of drivers on a rural road with no suspicion of any wrongdoing, solely because the road abutted a reservoir thought to be potential target for terrorism, were unconstitutional).

349 *See, e.g.*, Cassidy v. Chertoff, 471 F.3d 67 (2d Cir. 2006) (detailing and relying on extensive findings from the Department of Homeland Security about dangers to ferries and methods to ameliorate risks in endorsing warrantless searches of ferry riders traveling from Vermont to New York to combat possible terrorist attacks); Am.-Arab Anti-Discrimination Comm. v. Mass. Bay Transp. Auth., No. 04–11652–GAO, 2004 WL 1682859, at *4 (D. Mass. July 28, 2004) (permitting suspicionless searches of all buses passing by the Boston convention center where the Democratic National Convention was taking place, but only during the four-day period of the convention); *cf.* MacWade v. Kelly, 460 F.3d 260, 264–65, 273 (2d Cir. 2006) (emphasizing, in upholding the constitutionality of bag inspections of riders on the New York City subway system, the method by which the NYPD carried out the searches, including providing notice of the searches to all entering passengers, allowing individuals who did not wish to be searched to leave the system, and relying on a formula that ostensibly gave law enforcement personnel "virtually no discretion").

350 *See supra* Part I.B.3.

351 Bourgeois v. Peters, 387 F.3d 1303, 1311 (11th Cir. 2004).

352 *See, e.g.*, *infra* Parts III.C, F.

circumstances in which surveillance in public does not rise to the level of a search, meaning that it need not meet constitutional standards of reasonableness. However, where surveillance in public is transformed into a search according to the multi-part test articulated above, the special needs doctrine will rarely, if ever, save law enforcement from needing a warrant.

D. First and Fourteenth Amendment Claims

The discussion so far has focused on the elements that form the foundation for a Fourth Amendment claim, but one final point remains to be addressed. What happens when a protest, demonstration, or other public event occurs within a public space, and surveillance technologies that do not otherwise constitute a search intentionally focus on persons exercising their First Amendment rights? The Fourth Amendment may not be capacious enough to cover that activity, particularly in light of Supreme Court doctrine holding that the motive behind a stop or search is irrelevant to the Fourth Amendment analysis.[353]

That is not, however, the end of the constitutional inquiry. When surveillance is deliberately focused on the exercise of First Amendment rights or undertaken in retaliation for the exercise of such rights, whether or not any resulting harm is intended, the targets may have viable First Amendment claims in response.[354] In light of revelations that the federal government has monitored activists engaged in lawful activities in support of Black Lives Matter, for instance, this avenue is particularly salient.[355] In addition, when surveillance is disproportionately focused at particular racial, ethnic, or religious groups, claims

---

353 Whren v. United States, 517 U.S. 806, 812 (1996).

354 *See, e.g.*, Reporters Comm. for Freedom of the Press v. AT&T Co., 593 F.2d 1030, 1064 (D.C. Cir. 1978) ("[A]ll investigative techniques are subject to abuse and can conceivably be used to oppress citizens and groups, rather than to further proper law enforcement goals. In some cases, bad faith use of these techniques may constitute an abridgment of the First Amendment rights of the citizens at whom they are directed . . . .").

355 *See, e.g.*, George Joseph, *Exclusive: Feds Regularly Monitored Black Lives Matter Since Ferguson*, THE INTERCEPT (July 24, 2015, 2:50 PM), https://theintercept.com/2015/07/24/documents-show-department-homeland-security-monitoring-black-lives-matter-since-ferguson; *see also* Handschu v. Special Servs. Div., 288 F. Supp. 2d 411, 420–31 (S.D.N.Y. 2003) (limiting the NYPD's use of videotaping of demonstrations due to previous harassment for exercise of First Amendment rights); GLOBAL JUSTICE INFO. SHARING INITIATIVE, RECOMMENDATIONS FOR FIRST AMENDMENT-PROTECTED EVENTS FOR STATE AND LOCAL LAW ENFORCEMENT AGENCIES 4 (2011), https://www.ncirc.gov/onlinetraining/modules/first_amendment_rollcall/Recommendations.pdf (proposing best practices for law enforcement activity at First Amendment-protected events, including suggesting that "taking pictures and videos of the event" and "[c]ollecting . . . identifying information (such as license plates) of participants, people in the area, counterdemonstrators, or bystanders watching the event" would be a "red flag").

may be available under the Equal Protection Clause of the Fourteenth Amendment.[356]

The Third Circuit, for instance, recently considered allegations that the NYPD had spied on Muslim activists and community members because of their religious affiliation and activities, core interests protected by the First Amendment.[357] The NYPD was said to have targeted mosque attendees by taking pictures and videos, collecting their license plate numbers, and directing surveillance cameras at religious centers to identify the congregants, causing the plaintiffs to significantly curtail their religious activity.[358] In ruling that the plaintiffs could move ahead with their case, the court in *Hassan v. City of New York* was clear: discriminatory surveillance can cause real harms, and those harms can give rise to viable First Amendment claims.[359]

The court distinguished *Hassan* from *Laird v. Tatum*, a seminal 1972 Supreme Court case on the chilling effects of surveillance.[360] In *Laird*, a group of citizens challenged a surveillance and information-collection program that was implemented by the U.S. Army in the wake of the 1967 riots in Detroit and the assassination of Martin Luther King, Jr.[361] The plaintiffs could not show that the Army had taken any action against them,[362] however, and as the appeals court put it, "the information gathered is nothing more than a good newspaper reporter would be able to gather by attendance at public meetings and the clipping of articles from publications available on any newsstand."[363] In holding that they did not have standing to pursue their claim, the Supreme Court emphasized the vagueness of the allegations. A "subjective 'chill,'" based only on a fear that the information collected might be used against them in the future, was not sufficient; instead, the plaintiffs must show an actual injury.[364]

In *Hassan*, by contrast, the plaintiffs alleged that the NYPD was deliberately and covertly spying on them because of their religious identity and provided evidence that the surveillance had curbed their constitutionally-protected

---

356 *See* Hall v. Pa. State Police, 570 F.2d 86, 91 (3d Cir.1978) ("Although it may be assumed that the state may arrange for photographing all suspicious persons entering the bank, it does not follow that its criterion for selection may be racially based, in the absence of a proven compelling state interest." (citation omitted)).

357 Hassan v. City of New York, 804 F.3d 277 (3d Cir. 2015).

358 *Id.* at 288.

359 *Id.* at 291.

360 408 U.S. 1 (1972).

361 *Id.* at 2–5.

362 *Id.* at 13.

363 *Id.* at 9 (quoting Tatum v. Laird, 444 F.2d 947, 953 (D.C. Cir. 1971)).

364 *Id.* at 13–14.

religious activities, including discussing their faith and worshipping at their mosques.[365] The *Hassan* court observed that "*Laird* doesn't stand for the proposition that public surveillance is . . . *per se* immune from constitutional attack . . . ."[366] Because the plaintiffs had alleged that the NYPD's actions had caused them "direct, ongoing, and immediate harm," their First Amendment claims were justiciable.[367] The panel also emphasized that surveillance may not be targeted on the basis of race or other protected categories, suggesting that such surveillance would give rise to Equal Protection claims as well.[368]

Moreover, membership in a protected category (such as religion) is not necessary for a court to find that surveillance implicates the First Amendment; covert surveillance in retaliation for filing an employment discrimination claim can suffice.[369] As the Third Circuit observed in *Anderson v. Davila*, government retaliation in response to exercise of the "right to petition the government for grievances," a "protected activity under the First Amendment," is a "specific present harm."[370] The point was borne out in a case involving a Wikileaks volunteer whose electronic devices were seized at the U.S. border and retained by the government for a month and a half.[371] In *House v. Napolitano*, the court affirmed that simply because an initial search is constitutional under the Fourth Amendment does not mean that government agents may "target someone for their political association."[372]

Thus, where political activists or religious adherents are dogged by surveillance devices, be they cameras, drones, or other technologies, they will have viable First Amendment claims if the potential harm rises above a vague fear that the fruits of the surveillance may be used at some point in the future. For instance, where the surveillance is targeted on the basis of religion, race, or another protected category, or is undertaken in retaliation for other First Amendment activity, viable First Amendment claims would exist. This is true even if the surveillance merely deters association, protesting, or petitioning,

---

365 Hassan v. City of New York, 804 F.3d 277, 288 (3d Cir. 2015).

366 *Id.* at 292.

367 *Id.*; *see also* United States v. Gering, 716 F.2d 615, 620 (9th Cir. 1983) (upholding mail covers targeting minister at residence and church against First Amendment challenge in absence of showing that "mail covers were improperly used and burdened . . . free exercise or associational rights").

368 *Hassan*, 804 F.3d at 292 ("[I]n several post-*Laird* cases we have recognized that, while surveillance in public places may not of itself violate any privacy right, it can still violate other rights that give rise to cognizable harms." (footnote omitted)).

369 Anderson v. Davila, 125 F.3d 148, 162 (3d Cir. 1997).

370 *Id.* at 160, 164.

371 House v. Napolitano, No. 11-10852-DJC, 2012 WL 1038816, at *1–3 (D. Mass. Mar. 28, 2012).

372 *Id.* at *11.

rather than blocking these activities outright, and even if the government does not intend to cause specific harm. As the Supreme Court has observed, "associational rights 'are protected not only against heavy-handed frontal attack, but also from being stifled by more subtle governmental interference' and . . . these rights can be abridged even by government actions that do not directly restrict individuals' ability to associate freely."[373]

III. THEORY IN PRACTICE

This final Part offers several case studies to demonstrate how this approach would play out in the context of specific surveillance technologies. While the analysis will usually depend on the specific facts of the case (as do many Fourth Amendment inquiries), these case studies endeavor to respond to and refute the criticism that proponents of a more holistic approach to public space surveillance do not grapple with the "what-if"—that is, the logical next step of setting out when additional legal process would be required and how both the judiciary and law enforcement would know when the requirement has been triggered.[374]

A. GPS Trackers on Cars

After *United States v. Jones*, physically attaching a GPS tracker presumptively qualifies as a Fourth Amendment trespass.[375] The question that remains is how a court would analyze the use of GPS devices that are built-in or not otherwise attached by law enforcement.

Duration: GPS tracking covering at least fourteen days is likely to trigger constitutional scrutiny; such an extensive body of information can be used to create a mosaic that conveys detailed personal information, chilling First Amendment rights and risking exploitation by an unscrupulous governmental agency or official. Where the monitoring is for a shorter period, one guiding factor would be whether it is a period that would reasonably be expected to be accomplished by the police without the use of cutting-edge technologies. If it would not, then the duration should be placed on the search side of the scale.

Cost: GPS tracking is a paradigmatic form of surveillance that is many orders of magnitude less expensive than assigning officers to follow someone. By

---

373 Lyng v. Int'l Union, United Auto., Aerospace & Agric. Implement Workers of Am., UAW, 485 U.S. 360, 367 n.5 (1988).

374 *See* Kerr, *supra* note 170, at 346 ("It [is] particularly telling that not even the proponents of the mosaic theory have proposed answers for how the theory should apply.").

375 565 U.S. 400, 404 (2012).

"evad[ing] the ordinary checks that constrain abusive law enforcement practices," including "limited police resources," GPS upsets the usual curbs on government overreach.[376] The cost consideration should weigh strongly in favor of finding GPS tracking, particularly of any significant duration, to be a Fourth Amendment search.

Recording: GPS tracking will almost inevitably produce a record (such as the 2000-page readout produced in *Jones*[377]), facilitating both the ability to draw extensive inferences about the driver's life and associations and the opportunity to identify single, sensitive moments. The information will often be less richly detailed than that offered by real-time cell phone tracking, since it will identify where a person drove and parked but not necessarily the homes or businesses that he or she entered (or where she traveled by foot or public transportation). Nevertheless, if records indicate that a car is parked in front of a private home on multiple occasions, it is reasonable to infer that the subject has a relationship of some kind with people in the house. Where records reveal a person's travels throughout a day or a week, inferences can be drawn about where he or she lives, worships, has intimate relationships, and more.

Presence in private home: Unlike a cell phone or other device carried on the person, a car's GPS device generally will not reveal an individual's presence in a private home, and this factor generally would not contribute to a finding of a search. There are circumstances, however, in which a GPS could indicate this information. Where a car is parked night after night in the same driveway, for instance, a strong inference can be drawn—barring contrary information—that the driver lives in that home (or has a relationship with the occupant). Or a car might drive through a private gate and down a winding private road to a secluded ranch, obscured from view by trees. While the presence of a car in a rural area might, under normal circumstances, be discernible from air by a helicopter, a car surrounded by natural features that help to shield it from view would not be. GPS information, however, could reveal the location of the car. In that case—and regardless of the duration of surveillance—the disclosure of otherwise private information should be added to the ledger.

Erosion of core constitutional rights and combination of technologies: Neither of these factors is likely to come into play in the context of GPS tracking, at least in its current state. The analysis might change if, for instance, law

---

376 *Id.* at 956. (Sotomayor, J., concurring) (quoting Illinois v. Lidster, 540 U.S. 419, 426 (2004)).
377 *Id.* at 948.

enforcement tried to access an OnStar-type unit that recorded the content of conversations inside the car.

Conclusion: Given the significantly lowered cost of GPS monitoring and the creation of a recording, GPS monitoring of any appreciable duration is likely to constitute a Fourth Amendment search. Because governmental GPS tracking occurs almost exclusively for law enforcement purposes, police will be required to obtain a warrant in advance. In light of the preference for clear, bright-line rules to guide law enforcement, law enforcement agencies could require a warrant for any GPS use, or direct that tracking for any period above a set duration—say, six to eight hours—requires a warrant.[378]

Such a warrant would have to be tailored to focus on those locations for which there is probable cause to believe that there is a connection between the target and criminal activity. For instance, the warrant would need to target the particular routes the target is believed to take to engage in the criminal activity, or the locations of meetings between the target and suspected co-conspirators. "Geofencing" capabilities, which turn off tracking technology when the device leaves certain geographic boundaries, may be useful in this regard.[379]

B. Cell Phone Location Information

The dispositive feature of cell phone tracking, insofar as the Fourth Amendment is concerned, is that it can reveal information from inside a private home or other protected space that would otherwise be obtainable only with a warrant. To be sure, cell phones can also enable intrusive monitoring for long periods of time, at low cost, and create a recording of an individual's daily activities. But they are perhaps unique among the surveillance technologies for their ability to disclose their possessor's presence in a private home, regardless of the duration of tracking.[380] Moreover, law enforcement will rarely know in advance when the owner is about to enter a private area, and thus generally will not be able to cease tracking in advance to avoid capturing sensitive data.

---

[378] An agency could also take into account the likelihood that the GPS will reveal constitutionally protected information even in the absence of a long period of tracking. Thus, rural law enforcement agencies, serving residents who are more apt to retreat to private and inaccessible spaces that would be accessed only via GPS, might determine that a warrant is always the proper procedure in the absence of exigent circumstances.

[379] *See HTG Explains: What Geofencing Is (and Why You Should Be Using It)*, HOW-TO GEEK, http://www.howtogeek.com/221077/htg-explains-what-geofencing-is-and-why-you-should-be-using-it/ (last visited Oct. 31, 2016).

[380] *See, e.g.*, *In re* Application for Tel. Info. Needed for a Criminal Investigation, 119 F. Supp. 3d 1011, 1023 (N.D. Cal. 2015) ("Cell phones generate far more location data because, unlike the vehicle in *Jones*, cell phones typically accompany the user wherever she goes.").

Regardless of duration, therefore, cell phone surveillance should presumptively qualify as a Fourth Amendment search.

As with GPS tracking, a warrant for real-time cell phone tracking should be tailored to obtain information that will lead to evidence of a crime, rather than information about all places the person goes at all times of the day, every day. Such a warrant might restrict the times at which the phone is tracked and the length of tracking. Similarly, a warrant for historical cell site location information should be focused on times and places for which there is probable cause to believe there is evidence of a crime. Finally, a warrant for a Stingray should be designed to limit the collection of data about innocent third parties before the fact, as well as to purge any innocent persons' data soon after collection.

C. Fixed Surveillance Cameras

Once a surveillance camera is installed, it can be deployed for an array of purposes. Because surveillance cameras are most frequently installed for general public safety purposes, this case study will focus on using cameras to monitor public areas.[381]

Duration: The durational factor is analyzed with respect to a single individual—that is, whether a single person can be tracked for an appreciable duration. A small number of cameras trained on a public area are highly unlikely to monitor a single individual or group for an extended duration. Even where they capture a public event such as a marathon or a protest, the length of the surveillance is not likely to elevate it to a search. It is possible, of course, that a mounted surveillance camera could view, over an extended period, an individual who is carrying out an ongoing protest—for instance, the long-time (and now defunct) anti-war encampment near the White House.[382] If the surveillance cameras have a concrete chilling effect on the protestors, they may have a stand-alone First Amendment claim. In addition, if cameras are networked with cameras in other locations to allow for the easy tracking of an individual—systems that are already in place in the British cities of London and Sheffield,

[381] Where a camera is used for targeted tracking of an individual, the Fourth Amendment analysis will be highly fact-dependent, with the duration of tracking constituting a significant factor.

[382] Caitlin Gibson, *Connie Picciotto Has Kept Vigil Near the White House for 32 Years. Why, and at What Cost?*, WASH. POST (May 2, 2013), http://www.washingtonpost.com/sf/feature/wp/2013/05/02/connie-picciotto-has-kept-vigil-near-the-white-house-for-32-years-why-and-at-what-cost/.

with New York City not far behind[383]—the Fourth Amendment would require that there be policies in place to ensure that they are not used to track individuals without a warrant (save in exigent circumstances).

Cost: Where the cameras are doing the work of only several police officers, by monitoring a fairly small area, the cost may not be significantly less than deploying the officers themselves, particularly when the work of monitoring the cameras is taken into account.

Recording: Some cameras allow for monitoring in real-time, some record for later review, and some do both. When a camera records in a public square for later review, there are two concerns of potentially constitutional magnitude. The first, of less serious concern, is that an individual person could be captured multiple times on video if he or she regularly uses the square as a thoroughfare or a place to carry out personal affairs or business. This possibility does not trigger the durational consideration, however, as it still will not enable individualized tracking over a long period of time or the creation of a mosaic (unless the person literally conducts all of his or her business in and around the limited area of the public square).

Perhaps the more salient concern is the ability to pick out and identify individual, sensitive moments that would otherwise be lost to the natural passage of time. Where biometric recognition technologies are deployed, the risk becomes even more acute, as it becomes a simple matter to pick out a particular face, a tattoo, or a style of walk weeks or even months after a person strolled through the area. Not recording at all would, of course, eliminate this risk. Where recording is enabled, stringent back-end restrictions would mitigate the threat as a policy matter. For instance, limiting the length of recordings, the period of time for which the video is kept, and the purposes to which it can be put, and also prohibiting the use of automated recognition technologies without a warrant could all serve as appropriate limitations.[384] (As explained above, these back-end restrictions would not mitigate the threat as a constitutional matter, since the collection itself would still be unlimited.[385])

---

383 *See* NOAM BIALE, ACLU, WHAT CRIMINOLOGISTS AND OTHERS STUDYING CAMERAS HAVE FOUND, https://www.aclu.org/files/images/asset_upload_file708_35775.pdf (referencing London camera system); *Closed Circuit Television (CCTV)*, SHEFFIELD CITY COUNCIL, https://www.sheffield.gov.uk/in-your-area/report_request/crime/cctv.html (last edited Dec. 12, 2016); Kelly, *supra* note 83; *see also* Dees, *supra* note 247; Parascandola & Moore, *supra* note 247.

384 *See, e.g.*, THE CONSTITUTION PROJECT, GUIDELINES FOR PUBLIC VIDEO SURVEILLANCE (2007), http://www.constitutionproject.org/wp-content/uploads/2012/09/54.pdf.

385 *See supra* notes 381–84 and accompanying text.

Presence in private home: A surveillance camera directed at a relatively confined public area is unlikely to capture otherwise inaccessible information about a private home or other constitutionally-protected area. In ordinary circumstances, this factor will not contribute to a finding of a search.[386]

Erosion of core constitutional rights: Surveillance cameras may capture the exercise of First Amendment rights: peaceful assemblies and protests are a regular feature of some public squares, and where government buildings are included, the cameras may observe—and could chill—individuals' exercise of their First Amendment right to petition the government.[387] As a basic matter, however, individuals have not traditionally enjoyed protection against being observed by law enforcement at a protest, and the mere addition of technology in this case, without more, would not erode a historically recognized right.

Surveillance cameras in public areas could also be used to pick up the content of conversations. While surveillance cameras generally are not wired for sound, they could be used to monitor a conversation in sign language or to read the speakers' lips, even where the speakers sit close to each other and turn their bodies so as to bar interlopers or keep their voices low enough to be inaudible to outsiders.[388] Such surveillance would assuredly violate any reasonable expectation of privacy, even if it did not trigger the other factors.

Combination with other technologies: Surveillance cameras can be outfitted with supplementary technologies, including license plate readers and biometric recognition technologies. As explained below, the addition of a license plate reader for one-time reads would not elevate the use of the camera to a search if the data is not stored for future use. Advanced biometric recognition capabilities change the game more substantially, by impinging on the anonymity that many people take for granted, and their use will warrant more scrutiny.

Conclusion: Taken together, these factors suggest that erecting a limited number of cameras in a public space will not constitute a search if there are

386 Pole cameras aimed at a private backyard could, as the *Vargas* court observed, reveal an individual's movements in or near his home over a period of time in excess of what could reasonably be carried out by police officers. *See* Order Granting Defendant's Motion to Suppress, United States v. Vargas, No. CR-13-6025-EFS, at 22 (E.D. Wash. Dec. 15, 2014). I do not, however, include pole cameras in the universe of surveillance cameras in public space, since they are directed at a home's curtilage, which is historically protected by the Constitution as an adjunct to the home.

387 *See* U.S. CONST. amend. I ("Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.").

388 *See supra* Part III.B.5.

restrictions on recording and the cameras are not used for longer-term, networked tracking of individuals. Where one of these factors changes significantly, the overall analysis will change as well.

The fact that surveillance cameras enable a range of surveillance capabilities and are likely to become a permanent feature of the landscape calls for a thoughtful process before putting them up. In Washington, D.C., for instance, local legislation directs the chief of police to consider a set of enumerated factors in evaluating requests for cameras.[389] There must be community involvement at multiple stages, and the police department is obligated to comply with certain reporting requirements.[390] In exigent circumstances, a camera can be deployed without prior notice, but it must be removed when the circumstances are over and post-deployment notice must be provided.[391] This model suggests one method of engaging the community, limiting the use of cameras, and providing transparency about surveillance devices.

D. Drones for Public Safety

Duration: As with a surveillance camera, a drone that remains focused on a discrete public area is unlikely to capture any individual for more than a brief period of time. A drone may, however, have a much wider scope than a camera; depending on the height of the drone and the resolution of the camera, it could capture views of a whole neighborhood or even an entire town.[392] In addition, it is far easier to use a drone to track a single person, increasing the duration of individual surveillance.[393] Again, the inquiry would be a fact-intensive one,

---

389 *See* Use of CCTV to Combat Crime, 24 D.C. Reg. 2508.2 (directing the chief of police to consider "[t]he number and type of calls for service" and "[a]ny crimes that were committed in the proposed CCTV camera location," requests made by the relevant Advisory Neighborhood Commission or a community group, and "any other objectively verifiable information from which the Chief of Police may ascertain whether the health, safety, or property of residents who live in the proposed"). Requests for cameras can come from police officers, district commanders, or community groups, among others.

390 *See* Public Notification, 24 D.C. Reg. 2502.2 (requiring chief of police to provide notice and a range of information about the cameras to the public before the device is put up, including system capabilities, how cameras are used, length of deployment, and viewing area); Public Notification, 24 D.C. Reg. 2502.3; Public Notification, 24 D.C. Reg. 2502.7–9; METRO POLICE DEP'T, ENHANCED USE OF CCTV TO COMBAT CRIME 4 (Aug. 9, 2006) (requiring District commanders who are requesting cameras to detail the contacts they have had with relevant elected leaders (neighborhood commissioners and council members), and to justify the request).

391 Public Notification, 24 D.C. Reg. 2502.5.

392 Ellen Nakashima & Craig Whitlock, *With Air Force's Gorgon Drone 'We Can See Everything'*, WASH. POST (Jan. 2, 2011, 12:09 AM), http://www.washingtonpost.com/wp-dyn/content/article/2011/01/01/AR2011010102690.html.

393 *See, e.g.*, THOMPSON, *supra* note 93, at 16 ("[S]ome drones could theoretically 'stay in the air forever.' Unlike a stationary license plate tracker or video camera, drones can lock in on a target's every move for days,

depending on the surveillance that the police could be expected to undertake under the circumstances, but the addition of a drone makes it a much simpler matter to create a mosaic.[394]

Cost: The cost of using a drone is likely to vary according to the circumstances, and the comparative cost of monitoring a public area will depend significantly on the duration of surveillance. As against an already-mounted surveillance camera, for instance, it will presumably be more expensive to send and keep a drone aloft than simply watching an existing camera. As against a team of officers, however, the comparative cost will depend on the drone's capabilities: a single drone watching a relatively limited area may not be much more expensive than sending an officer to do the same job, while a drone that can travel to high elevations to get a view of a large public area and zoom in to get small-scale details may be able to do the job of a group of officers at far less expense.

Recording: A drone hovering above a public space is almost certain to be recording; the presence or absence of a recording would be added to the ledger as appropriate.

Presence in private home: As with the other factors, this element of the inquiry is likely to be quite fact-dependent, depending upon the drone's capabilities. A drone with viewing capabilities restricted to a relatively limited public space (whether by policy or technology) is unlikely to glean information about the inside of a home. On the other hand, a drone with the capacity to survey a large area in high resolution may be able to simultaneously monitor a public space and watch the goings-on inside a home, and a smaller drone could simply leave the public space and peer inside a home, as a drone memorably did outside Senator Dianne Feinstein's home (leading her to call for a warrant requirement

---

and possible weeks and months. This ability to closely monitor an individual's movements with pinpoint accuracy may raise more significant constitutional concerns than some other types of surveillance technology.").

394 Similarly, where drones are used for targeted tracking, the warrant requirement should come into play more quickly than for surveillance cameras, since drones allow for more precise tracking, in places where an officer may not be able to go, and are able to "see" inside a home more easily. *See, e.g.*, ELEC. PRIVACY INFO. CTR., *supra* note 246 ("Surveillance drones are equipped with sophisticated imaging technology that provides the ability to obtain detailed photographs of terrain, people, homes, and even small objects. Gigapixel cameras used to outfit drones are among the highest definition cameras available, and can 'provide real-time video streams at a rate of 10 frames a second.' On some drones, operators can track up to 65 different targets across a distance of 65 square miles."); Kathryn A. Wolfe, *Feinstein: Drone Inches from Face*, POLITICO (Jan. 15, 2014, 4:15 PM), http://www.politico.com/story/2014/01/senator-dianne-feinstein-encounter-with-drone-technology-privacy-surveillance-102233 (reporting on drone hovering outside Senator Feinstein's house).

for drones).[395] The actual capabilities of the drone in question will guide the court's analysis in this realm.

Significantly, unlike with cell phones and GPS devices, where the target himself holds the tracking device and law enforcement may have no way to anticipate or avoid obtaining information from inside a home, law enforcement agents will be piloting the drone and could avoid approaching a private area in a manner that would intrude on constitutionally protected rights. Where law enforcement knows in advance that their drone use may invade otherwise constitutionally protected space, they should seek a warrant at the outset (or take steps to avoid approaching a protected space).

Erosion of core constitutional rights and combination of technologies: If a drone carries a technology that can pick up the content of conversations, or if an additional device such as a license plate reader or cell phone tracker is installed in the drone, then courts should take account of that in their analysis.

Conclusion: The combination of these factors—the ease with which a drone can transition from general surveillance to individualized tracking and the intrusive nature of mobile drone surveillance, among others—suggests that a default warrant requirement for law enforcement drone use, whether for investigative tracking or for public safety, would most vigorously protect Fourth and First Amendment rights. In the absence of clear law, some states are taking precisely this approach. Virginia's Governor, for instance, recently signed a bill requiring a warrant any time a law enforcement agency uses a drone, whether for a criminal investigation or more generalized surveillance, and there have been similar efforts in other states.[396] Such a warrant could incorporate a geofence to prevent the drone from straying outside prescribed boundaries, making its range more akin to that of a surveillance camera, and altitude

---

[395] Wolfe, *supra* note 394.

[396] Unmanned Aircraft Systems; Use by Public Bodies During Execution of a Search Warrant, Exception, S. 1301, 2015 Gen. Assemb., Reg. Sess. (Va. 2015) (enacted); Tim Cushing, *Virginia Governor Signs Warrant Requirement For Police Drone Use; Balks At Seven-Day Limit On ALPR Data Retention*, TECH DIRT (May 7, 2015, 3:47 PM), https://www.techdirt.com/articles/20150507/08315130923/virginia-governor-signs-warrant-requirement-police-drone-use-balks-seven-day-limit-alpr-data-retention.shtml; Zusha Elinson, *Brown Vetoes Bill Requiring Warrants for Drone Surveillance*, WALL ST. J. (Sept. 29, 2014, 6:15 PM), http://www.wsj.com/articles/california-governor-vetoes-bill-requiring-warrants-for-drone-surveillance-1412007285 (noting that a similar bill passed the California legislature with bipartisan support but was vetoed by Governor Brown); Christopher Keating, *Police Would Need Warrant to Launch Surveillance Drones*, HARTFORD COURANT (Apr. 7, 2015, 5:57 PM), http://www.courant.com/politics/hc-drone-bill-passed-0408-20150407-story.html (Connecticut); Michael Phillis, *Bill Governing Law Enforcement's Use of Drones Advances*, PHILLY VOICE (May, 15, 2015), http://www.phillyvoice.com/bill-governing-police-use-drones-advances/ (New Jersey).

restrictions could be imposed up front to prevent a drone from executing pervasive, widespread surveillance (or low-level, intrusive surveillance).

E. Automatic License Plate Readers

Duration: If the reader runs a plate or plates and then discards any plate that doesn't result in a "hit," the duration of surveillance is essentially negligible. If it sends the data to a database for retention, however, the duration may be much longer. When license plates are routinely scanned by multiple readers and the information is retained in a database for an appreciable period, the combined mosaic effect of that location information can be used to yield far more personal information than a single reading at a single point in time. A longer-term database of automobile movements will have First Amendment implications as well, whether the database is used to obtain multiple points of information about a single car or to place multiple cars in the same place at various times, suggesting patterns of association.

Cost: An automated license plate reader accomplishes collection and analysis of information with a speed that would otherwise require a team of officers at multiple points across a city and even across the country. Because it carries out its mission through lightning-fast reading, translation, transmission, and analysis of every plate that passes its station, achieving the same goals in a non-automated fashion would be not only prohibitively expensive but also essentially impossible. The cost factor thus weighs strongly in favor of a search determination.

Recording: License plate readers can record information; the more they record and the longer they keep the data, the greater the threats to individuals' privacy. Recording more information should lead to a stronger presumption in favor of a search.

Presence in private home: Most stationary license plate readers will not detect information about a private home, as they are usually mounted in busier urban areas, on thoroughfares in and out of town, etc. Readers could be mounted in residential neighborhoods, however, or on patrol cars that drive through residential areas. In one well-publicized example, a passing police car equipped with a license plate reader took a picture of a car in a private driveway that captured not only the license plate but an image of the owner and his two small

children stepping out of the vehicle.[397] This factor generally will not tip in favor of a search finding, but a court would need to examine the particular circumstances.

Erosion of core constitutional rights and combination of technologies: These factors appear less likely to be salient when it comes to license plate readers.

Conclusion: This analysis suggests that when license plate readers store information in a database for retention, as opposed to running plates against a hot list and immediately discarding the plates that do not match, the use of the reader is a search. Such storage is incontrovertibly for law enforcement purposes: the reader collects information to aid law enforcement in finding offenders and pursuing them for restitution or imprisonment. Fourth Amendment doctrine would thus demand a warrant.

Using license plate readers to collect information about every car driving past every license plate reader in the country, however, is incompatible with the individualized suspicion and particularity requirement of the Fourth Amendment, and thus cannot be saved even with a warrant.[398] Readers should be used only for checks against hot lists, only if the information is immediately purged, and only if there are careful restrictions and protections in place to guard against abuse.

F. Body-Worn Cameras

Body-worn cameras are different from most of the other surveillance technologies discussed here because, unlike the other technologies canvassed in this article, they do not (at least in their current iteration) amplify the scope of surveillance. That is to say, the camera sees only what the police officer sees, and the camera is dependent upon the officer. In addition, the typical police officer on a beat will have interactions with a range of individuals over the course of her week; an officer generally does not interact with, and record, the same person for days on end.

Body cameras nevertheless raise both constitutional and policy concerns that warrant close attention to their use and detailed guidelines when they are deployed. While a detailed policy discussion is beyond the scope of this Article,

---

[397] *See* Ali Winston, *License-Plate Readers Let Police Collect Millions of Records on Drivers*, CTR. FOR INVESTIGATIVE REPORTING (June 26, 2013), http://cironline.org/reports/license-plate-readers-let-police-collect-millions-records-drivers-4883.

[398] *See supra* Part II.C.1.

the treatment below analyzes body cameras in the context of the multi-part Fourth Amendment test and suggests some practical considerations.

Duration: An individual body-worn camera typically will not enable long-term surveillance; even if the camera records constantly, it will still be for no longer than an individual police officer could observe a person or gathering, since the camera will be affixed to an officer. Videos from multiple body-worn cameras could be knitted together to create a mosaic, however, and could be augmented with footage from other sources and biometric recognition technology. The analysis will thus depend on the particular facts in question, but a single body-worn camera recording is unlikely to trigger this factor.

Cost: The actual costs of police surveillance are the same with a body camera or without; the individual officer is still walking the same beat, driving the same route, and responding to the same calls, with all the expenses in personnel and equipment that entails, whether she is equipped with a body camera or not. The main contribution of the body camera is to produce a video record, as described below. Body cameras are likely to lower other costs; where a defendant is caught on camera clearly committing a crime, for instance, he or she may plead guilty without going through the expense of a trial, and where a police officer is revealed to have engaged in misconduct, settlements and policing reforms may be achieved more quickly. But those costs are not salient to the preliminary question of whether the use of the camera itself constitutes a search. Real-time surveillance is no more or less expensive with a body camera attached.

Recording: By design, body cameras record when they are activated. Current body camera designs primarily rely on the police officer to activate it, but cameras that activate automatically in response to certain stimuli are already in development and, in some places, on the streets.[399] While the recordings may be relatively limited in duration (at least with respect to the length of time a given individual or group is captured), they may still create a "time machine" that would allow for the retrieval of sensitive information or a moment that would otherwise be anonymous.

---

[399] *See Digital Ally Receives VuLink Patent, Provides Automatic Body Cam Activation & In-Car Video System Linking*, EMS1.COM (Sept. 2, 2014), http://www.ems1.com/ems-products/cameras-video/press-releases/1977201-Digital-Ally-Receives-VuLink-Patent-Provides-Automatic-Body-Cam-Activation-In-Car-Video-System-Linking/; Ryan Mason, *More Than a Body Cam*, POLICE (Apr. 28, 2015), http://www.policemag.com/channel/technology/articles/2015/04/more-than-a-body-cam.aspx; Robert Maxwell, *Lakeway Police First to Use Automatic Body Cameras*, KXAN-TV (June 12, 2015, 4:57 PM), http://kxan.com/2015/06/12/lakeway-police-first-to-use-automatic-body-cameras/.

That said, this concern is somewhat lessened when it comes to video of the civilian with whom the officer is interacting. That interaction is hardly a private, anonymous moment, since it is by definition being observed by a law enforcement official already. Passersby may, however, object to being caught incidentally on video. These concerns would counsel, as a policy matter, in favor of redacting their faces and other identifying features if video is released publicly, and would also counsel in favor of restricting the retention period of video that is not evidence in a criminal case to a duration tied to the statute of limitations for filing a civilian complaint.

Presence in private home: One of the most sensitive issues surrounding body cameras is their use inside a private home. Most policies currently in force provide for body cameras to remain on when police enter a private home, whether in response to a call or because they are pursuing an escaping suspect.[400] A minority of policies direct officers, when possible, to obtain consent of the residents and to abide by a resident's request to turn off the camera.[401]

Many of the same factors that counsel in favor of body cameras—increased oversight of officer behavior, transparency regarding police-civilian interactions—would generally suggest that cameras should record inside a home as well, where it is even less likely that an outside observer would be in a position to witness police (or civilian) abuse. Moreover, an officer inside a home will generally have reason to be present, whether because she is executing a warrant or because she has responded to a call for service. The body camera's recording is therefore unlike tracking of a cell phone, which captures information from inside a home in the absence of a police officer who is authorized to be there.

At the same time, officers are not always inside a home for lawful reasons; examples of police entries in error abound.[402] In addition, a body camera

---

[400] *See, e.g.*, CHI. POLICE DEP'T, BODY WORN CAMERAS, S03-14 (2016), http://directives.chicagopolice.org/directives/data/a7a57b38-151f3872-56415-1f38-89ce6c22d026d090.html; SAN DIEGO POLICE DEPARTMENT PROCEDURE (2016), https://www.sandiego.gov/sites/default/files/149.pdf; *see also Police Body Camera Policies: Privacy and First Amendment Protections*, BRENNAN CTR. FOR JUSTICE (Aug. 3, 2016), http://www.brennancenter.org/analysis/police-body-camera-policies-privacy-and-first-amendment-protections.

[401] *See, e.g.*, ORLANDO POLICE DEPARTMENT POLICY AND PROCEDURE 1140.0, MOBILE VIDEO RECORDING SYSTEMS (2014), https://rcfp.org/bodycam_policies/FL/Orlando_BWC_Policy.pdf; SEATTLE POLICE DEP'T, BODY-WORN VIDEO PILOT PROGRAM, 16.091 (Apr. 1, 2015), http://www.seattle.gov/police-manual/title-16---patrol-operations/16091---body-worn-video-pilot-program.

[402] *See, e.g.*, Associated Press in Atlanta, *Georgia Police Shoot Man and Kill His Dog After Responding to Wrong House*, THE GUARDIAN (Sept. 1, 2015, 5:59 PM), http://www.theguardian.com/us-news/2015/sep/01/georgia-police-shoot-man-kill-dog-wrong-house; Vicki Brown, *Man Dies in Police Raid on Wrong House*, ABC NEWS, http://abcnews.go.com/US/story?id=95475&page=1 (last visited Nov. 1, 2015); Nick Ochsner,

captures a permanent record of the home and preserves it for later review, far different from the usual scenario of a police officer entering a home for a specified purpose and leaving at the close of the episode, without carrying out a videotape of everything he or she has observed.

Finally, a body camera may record sensitive moments such as an officer's interaction with a victim of domestic violence. This can be powerful evidence in support of prosecution in a domestic violence case, but it can equally dissuade a victim from speaking to a police officer or even calling an officer to her home.

Where an officer is an invitee to a home and the resident is aware of the body camera and does not request that it be turned off, its use would not appear to be a search. When the officer is in the home pursuant to the occupant's consent and he or she does request that the camera be turned off, the request must be honored; otherwise, the officer has exceeded the scope of the consent and his presence in the home is transformed into a warrantless, illegal search.

In general, the multiplicity of considerations above counsels in favor of caution and in favor of thoughtful, detailed polices regarding the circumstances in which cameras may record inside a private home and the ability for victims and others to request that the camera be turned off.

Erosion of core constitutional rights: Some research suggests that when police officers don body cameras, the incidence of "socially desirable behavior" goes up.[403] This is a beneficial result in many ways, if incidences of violence go down and courteous interactions increase. This effect may also, however, bear on the free exercise of First Amendment rights, particularly including political protest, which depends to some extent on the latitude to engage in behavior outside of social norms. In this regard, the effect may, ironically, be mitigated to some degree by the fact that the presence of police officers always imposes some chilling effect; the addition of a body camera adds to that chill, but perhaps not as much as long-term surveillance enabled by the technologies above. Notably, body cameras may also help *safeguard* some historically protected rights, including the right to be free from unequal treatment on the basis of race,

---

Albemarle PD Raids Wrong House, Residents Claim Damaged Property, WBTV (Nov. 3, 2015, 5:15 PM), http://www.wbtv.com/story/30421120/albemarle-pd-raids-wrong-house-residents-claim-damaged-property.

[403] POLICE FOUND., SELF-AWARENESS TO BEING WATCHED AND SOCIALLY-DESIRABLE BEHAVIOR: A FIELD EXPERIMENT ON THE EFFECT OF BODY-WORN CAMERAS ON POLICE USE-OF-FORCE (2013), https://www.policefoundation.org/publication/self-awareness-to-being-watched-and-socially-desirable-behavior-a-field-experiment-on-the-effect-of-body-worn-cameras-on-police-use-of-force/.

by adding an extra layer of accountability and oversight to the daily practice of policing. This category is thus a mixed bag.

Conclusion: Based on the factors above, the use of body-worn cameras does not appear to rise to the level of a Fourth Amendment search when they operate independently. If the status quo changes—if the cameras are linked to form a network, for instance, or if they are outfitted with biometric recognition technology—the analysis could shift as well.

Moreover, regardless of the constitutional outcome, the use of body-worn cameras does raise privacy concerns, since they record moments that would otherwise be ephemeral; this is both their value and their drawback. Body-worn cameras raise complicated questions regarding the privacy of multiple parties—officers, victims, and suspects—and might make sources more hesitant to speak to police officers confidentially. In addition, while officers may need to exercise judgment about when to turn a camera on and off—when speaking to a victim of domestic violence, for instance, or while speaking with a possible witness to a shooting who fears repercussions to herself—officer discretion over the operation of the camera threatens to undermine its effectiveness if officers are permitted to selectively record certain elements of an interaction.[404]

Accordingly, police departments should—as a policy matter, if not a constitutional one—have robust policies in place before deploying body-worn cameras, even in a pilot program. These policies should include guidelines regarding: when a camera may be turned on or off; whether officers must notify each member of the public they interact with that they are fitted with a body camera; how to handle video from a private residence; how to provide residents who have invited an officer into their home with an opportunity to request that the camera be turned off; the length of time for which non-evidentiary video recordings may be kept; and circumstances under which the video can be accessed both internally and by the public. Community input into the development of these policies is essential to ensure that any concerns are aired and the cameras meet the needs of the community.

---

[404] *See, e.g.*, Mateescu, Rosenblat & Boyd, *supra* note 120 (providing an overview of current state of play regarding body-worn cameras and cataloguing questions about police camera programs on civil rights and civil liberties); Martin Kaste, *Police Departments Issuing Body Cameras Discover Drawbacks*, NPR (Jan. 22, 2015, 6:57 PM), http://www.npr.org/blogs/alltechconsidered/2015/01/22/379095338/how-police-body-camera-videos-are-perceived-can-be-complicated; Jay Stanley, *Police Body-Mounted Cameras: With Right Policies in Place, a Win for All*, ACLU (Mar. 2015), https://www.aclu.org/technology-and-liberty/police-body-mounted-cameras-right-policies-place-win-all.

In addition, body cameras are likely to produce a rich store of data, even if they are only turned on at designated times, and some video will need to be retained for enough time to allow a citizen to make a complaint or a crime captured on camera to be investigated and prosecuted. Back-end restrictions, stringent oversight, and close attention to protections for First Amendment activities will therefore be particularly critical.

Finally, a body camera with biometric recognition capabilities is a significant technological enhancement, allowing the police officer to "see" more than she could otherwise, and could be far more susceptible to abuse.[405] Any policy on body cameras should address and strictly limit the use of biometric recognition technologies.

CONCLUSION

New technologies have changed the landscape of policing and surveillance. What once took significant manpower can now be accomplished at the click of a button. In the coming years, new technologies that are beyond our current imaginings will surely be pressed into use.

Civilians and law enforcement alike benefit from the steady innovation of new technologies and new applications. At the same time, these developments can enable surveillance of a depth, and with an ease, that was simply unimaginable even twenty years ago. There is a growing judicial consensus that this state of affairs profoundly implicates the Fourth Amendment protections that are fundamental to Americans' individual rights, including the right to some modicum of privacy and the right to associate, to speak, and to protest. At present, however, this consensus is still somewhat unfocused, with courts groping for firm principles to underpin their instincts. The six-part framework outlined here would offer guideposts for courts undertaking that inquiry.

Would a bright-line rule be simplest? Undoubtedly, yes. But a bright-line rule would also be woefully insufficient, excluding multiple circumstances in which structural privacy and resource constraints would guarantee privacy and even anonymity, and for which there is thus a strong instinct (judicial and otherwise) in favor of constitutional protection. This Article instead offers an

[405] This scenario is dependent upon facial recognition technology that is more sophisticated than the technology currently known to be available, which generally relies on ideal visual circumstances that do not exist on the ground.

articulable and relatively predictable framework to assist in moving Fourth Amendment protections into the digital age.