

Ruth Bader Ginsburg

Inn of Court

November 2016

Pupillage Group

***4th Amendment &
Electronic
Surveillance***

ARTICLES

THE FOURTH AMENDMENT FUTURE OF PUBLIC SURVEILLANCE: REMOTE RECORDING AND OTHER SEARCHES IN PUBLIC SPACE

MARC JONATHAN BLITZ*

Public video surveillance is changing the way police fight crime and terrorism. This was especially clear in the aftermath of the Boston Marathon bombing when law enforcement found images of the two suspects by analyzing surveillance images gathered by numerous public and private cameras. Such after-the-fact video surveillance was equally crucial to identifying the culprits behind the 2005 London subway bombing. But the rise of camera surveillance, as well as the emergence of drone-based video monitoring and GPS-tracking methods, not only provides an important boon for law enforcement, but also raises a challenge for constitutional law: As police gain the ability to technologically monitor individuals' public movements and activities, does the Fourth Amendment's protection against "unreasonable searches" place any hurdles in their way?

In the 2012 case, United States v. Jones, five justices, in two separate concurrences, signaled that it does—at least when the monitoring becomes too intense or prolonged. Their suggestion, however, raises two significant problems. First, it provides no principled basis for marking the point at which public surveillance morphs from a means by which police monitor public space

* Professor, Oklahoma City University School of Law. B.A., 1989, Harvard College, Ph.D. (Political Science), 2001, University of Chicago; J.D., 2001, University of Chicago. Thanks to Danielle Citron, Susan Freiwald, David Gray, Jim Harper, Stephen Henderson, Barry Johnson, Hannibal Kemerer, Ian Kerr, Orin Kerr, Art LeFrancois, Christopher Slobogin and Peter Swire for comments on the arguments in this Article. Thanks also to the organizers and audience of The Drones to Jones panel at the 2012 Privacy Law Scholars conference.

into a Fourth Amendment “search.” Under the “mosaic theory” embraced by the D.C. Circuit, such surveillance becomes a search only when it captures enough data points from an individual’s public life to construct a detailed picture (or “mosaic”) of her movements and associations. But how detailed may such a picture be before it is too detailed? Do police engage in a search simply by watching someone continuously, even if they do so without drones, GPS units, or other advanced technology? Second, the concurring opinions do not explain why the Fourth Amendment, if it does cover public surveillance of this kind, does not also cover the information-collecting police do when they simply watch a pedestrian or a driver. As Justice Scalia wrote in Jones, “Th[e] Court has to date not deviated from the understanding that mere visual observation does not constitute a search.” But if police collect the same information from watching a driver as they do from tracking him with GPS technology, why would their watching not also be a search?

This Article proposes a solution to each of these challenges by offering a two-part definition of a Fourth Amendment “search” in a public space. Police engage in a search when they (1) not only observe, but also record, images or sounds of people or events outside police presence; or (2) magnify details on a person or documents or other items the person is carrying and thereby reveal information that would not otherwise be apparent without a pat-down or a stop-and-search of a person’s papers or effects.

This technology-based or design-based definition of what constitutes a “search” avoids the problems that arise when the Fourth Amendment analysis regarding what constitutes a “search” is based on an investigation’s duration or intensity. Under the technology-based or designed-based definition, police engage in a search as soon as they begin recording remote events or magnifying otherwise invisible details, whether they have done so for two minutes or two weeks. Additionally, under this approach, Fourth Amendment constraints only apply to surveillance that goes beyond unadorned visual surveillance. This test is more workable and more in accord with Fourth Amendment logic. Recording is a search because, more than any other element of public surveillance, it allows police to engage in dragnet-style investigation of all activities in a public space. By transforming ephemeral occurrences into permanent records, recording allows government officials to search public lives frame by frame, much like they might search documents file by file. Certain types of magnification could also constitute a search because, just as a telescope focused on a home may be functionally equivalent to a home entry and search, certain types of magnification may be functionally equivalent to a physical search of persons, papers, or effects.

TABLE OF CONTENTS

Introduction.....	23
I. The Nature of the Problem and the Supreme Court's Initial Steps Toward a Solution.....	33
A. The Problem of Public Surveillance.....	33
B. A Simple, but Flawed, Position: Treating Open Areas as a Fourth Amendment Free Zone	38
C. The Supreme Court's Signals About Fourth Amendment Protection in Public Spaces.....	44
II. Another Solution: Recording and Magnification Searches	48
A. Constitutionalizing Public Surveillance: The Proposed Test.....	48
B. Recording as a Dividing Line Between Searches and Non-Searches.....	55
C. Extensions: When Magnification—and Recording— Should Count as Searches and When They Should Not...	62
III. Objections, Alternatives, and Limits: Different Ways of Defining a “Search” (and a “Reasonable Search”) in Public ...	68
A. The Objection that the Test Leaves Police Needing Greater Freedom To Investigate.....	68
B. The Objection that the Test Leaves Government with Too Much Opportunity for Unjustified Surveillance	71
1. Expanding the definition of a “search” to cover other privacy intrusions by government	71
2. More general technology-centered approaches.....	77
Conclusion	84

INTRODUCTION

Public surveillance technology is changing the way police fight crime and terrorism. This was clear in the aftermath of the Boston Marathon bombing when law enforcement quickly found images of the two suspects by “sift[ing] through a mountain of footage” gathered by public and private cameras.¹ It was also clear in the aftermath of the 2005 London subway bombings, when the suspects were quickly identified using video surveillance.² Touting these breakthroughs, cities have rushed to embrace camera systems, especially in the years after the 9/11 attacks.³ Police in Washington,

1. 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/index.html>.

2. ROY COLEMAN & MICHAEL McCABILL, *SURVEILLANCE & CRIME: KEY APPROACHES TO CRIMINOLOGY* 99 (2011).

3. See Jeremy Brown, *Pan, Tilt, Zoom: Regulating the Use of Video Surveillance of Public Places*, 23 BERKELEY TECH. L.J. 755, 761–62 (2008) (explaining that “[p]olice

D.C.;⁴ Chicago;⁵ and New York⁶ can now use camera networks to track a person strolling down the street. They can magnify and video record her movements, actions, and the details of her vehicle's license plate, or the items she is carrying out of a store.⁷ In fact, government officials do not have to make do with cameras mounted on lampposts or buildings. They can watch and record citizens from drones that hover in the skies and glide at the command of a distant operator to a new and better vantage point.⁸

This revolution in surveillance techniques not only provides an important boon for law enforcement. It also raises an important challenge for constitutional law. As police gain the ability to monitor citizens' public movements and activities with increasingly powerful cameras, does the Fourth Amendment's protection against "unreasonable searches" place any hurdles in their way? Do police need to obtain a warrant based on probable cause or to satisfy some other constitutional test of reasonableness before they use a drone to track a person's movements or reconstruct those movements using video footage from public cameras?

have praised video surveillance as an effective tool" and have increasingly employed more sophisticated surveillance).

4. See Mary Beth Sheridan, *D.C. Forging Surveillance Network*, WASH. POST (May 1, 2008), http://articles.washingtonpost.com/2008-05-01/news/36809706_1_security-cameras-closed-circuit-cameras-council-member (discussing centralization of the D.C. surveillance camera system, which will integrate "4,500 cameras trained on schools, public housing, traffic and government buildings" and allow "round-the-clock monitoring of the closed-circuit video systems run by nine city agencies").

5. See William M. Bulkeley, *Chicago's Camera Network Is Everywhere*, WALL ST. J. (Nov. 17, 2009), <http://online.wsj.com/article/SB10001424052748704538404574539910412824756.html> ("A giant web of video-surveillance cameras has spread across Chicago, aiding police in the pursuit of criminals but raising fears that the City of Big Shoulders is becoming the City of Big Brother.").

6. See Greg Botelho, *New York's Times Square: Always a Target, Always Watched*, CNN (Apr. 25, 2013, 9:28 PM), <http://www.cnn.com/2013/04/25/us/new-york-boston-attack> (noting that a "host of cameras" watches Times Square and other areas in New York and that among them are cameras that "capture 360-degree images," "shoot from above," or provide "ground-level surveillance footage").

7. See, e.g., *Chicago's High-Tech Cameras Spark Privacy Fears*, PHYS.ORG (Feb. 8, 2011) <http://www.phys.org/news/2011-02-chicago-high-tech-cameras-privacy.html#nRlv> ("At least 1,250 of [Chicago's cameras] are powerful enough to zoom in and read the text of a book. The [camera] system is also capable of automatically tracking people and vehicles out of the range of one camera and into another and searching for images of interest like an unattended package or a particular license plate.").

8. See Tom Reeve, *UAV Video Surveillance Drones Prepped for Take-Off*, SECURITY NEWS DESK (Feb. 2012), <http://www.securitynewsdesk.com/2012/02/03/uav-video-surveillance-drones-prepped-for-take-off> ("Drones . . . may soon be filling our skies, engaged in myriad video surveillance tasks.").

Only a few years ago, most courts and lawyers would have answered “no.”⁹ The Fourth Amendment protects people—and their “houses, papers, and effects”—from being subject to “unreasonable searches and seizures” by government officials.¹⁰ Supreme Court Justices as well as legal scholars have generally interpreted this provision as protecting individuals in the home, or some other space that is objectively and reasonably private or personal.¹¹ The Fourth Amendment bars the government, for example, from spying upon citizens in their living rooms and bedrooms; prying into their wallets, purses, or other closed “containers”; and opening sealed envelopes or closed drawers to read their private letters and diaries.¹² More generally, as Justice Harlan emphasized in *Katz v. United States*,¹³ the government generally does not need a warrant any time it watches us, but only when it observes us or examines our belongings after entry into places or circumstances in which we have a “reasonable expectation of privacy.”¹⁴

By contrast, the open and public space that we share with others—in streets, public squares, and parks—is not a private environment. We cannot exclude fellow citizens from this space nor command them to close their eyes and ears to what is going on around them. For example, when a person drives on a highway, she might be seen or even followed by other drivers, and some of these other drivers might be police officers. The Supreme Court held in *United States v.*

9. See, e.g., *United States v. Cuevas-Perez*, 640 F.3d 272, 274, 276 (7th Cir. 2011) (holding that GPS surveillance on public roads is not a search), *vacated*, 132 S. Ct. 1534 (2012) (mem.); *United States v. Marquez*, 605 F.3d 604, 609–10 (8th Cir. 2010) (same); *United States v. Pineda-Moreno*, 591 F.3d 1212, 1214, 1217 (9th Cir. 2010) (same), *vacated*, 132 S. Ct. 1533 (2012) (mem.); *United States v. Garcia*, 474 F.3d 994, 998 (7th Cir. 2007) (same); *United States v. Gonzalez*, 328 F.3d 543, 548 (9th Cir. 2003) (explaining that the Fourth Amendment does not protect “activities already visible to the public”).

10. U.S. CONST. amend. IV.

11. See, e.g., *Oliver v. United States*, 466 U.S. 170, 180–81 (1984) (finding that, while the Fourth Amendment limits police investigation of homes and the curtilage surrounding the home, it has no application to “open fields”); Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1010 (2010) (explicating that the Fourth Amendment does not protect conduct that is out in the open, while entering an enclosed space is usually a search).

12. See, e.g., *California v. Acevedo*, 500 U.S. 565, 598 (1991) (White, J., dissenting) (“Every citizen clearly has an interest in the privacy of the contents of his or her luggage, briefcase, handbag or any other container that conceals private papers and effects from public scrutiny. That privacy interest has been recognized repeatedly in cases spanning more than a century.”). As explained below, individuals do receive Fourth Amendment protections from searches in the cars, purses, rented lockers, or other areas in public space from which they can exclude outside observers, but this does not give them protection from monitoring of their activities in the open. See *infra* text accompanying notes 93–100.

13. 389 U.S. 347 (1967).

14. See *id.* at 360–61 (Harlan, J., concurring).

*Knotts*¹⁵ that individuals have no reasonable expectation of privacy in their movements on public roadways.¹⁶ Thus, people cannot raise Fourth Amendment complaints when their actions are open to the public, including law enforcement officers, even if these officers use hidden location-tracking devices or other technology to do so.¹⁷ While people may create some measure of constitutionally protected privacy, even in public spaces, by closing their car doors or keeping documents and other items inside a briefcase, purse, or some other container,¹⁸ people cannot constitutionally shield the actions they leave visible or audible. As one judge said in a recent Global Positioning System (GPS) tracking case: “The practice of using . . . devices to monitor movements on public roads falls squarely within the Court’s consistent teaching that people do not have a legitimate expectation of privacy in that which they . . . leave open to view by others.”¹⁹

Or so the Supreme Court and other courts insisted—until a year ago. In the 2012 case of *United States v. Jones*,²⁰ five Justices, in two separate concurring opinions, indicated that it is time for a doctrinal change.²¹ These five justices suggested that an important constitutional line is crossed—and the constraints of the Fourth Amendment are triggered—when public surveillance becomes too intense or prolonged.²² Justice Alito, for example, argued that, while “relatively short-term monitoring of a person’s movements on public streets” is generally free from Fourth Amendment restriction, “use of longer term GPS monitoring in investigations of most offenses

15. 460 U.S. 276 (1983).

16. *Id.* at 281.

17. *See id.* at 282.

18. *See California v. Acevedo*, 500 U.S. 565, 598 (1991) (White, J., dissenting) (restating that all citizens have a clear privacy interest in the contents of personal articles).

19. *United States v. Cuevas-Perez*, 640 F.3d 272, 276 (7th Cir. 2011) (Flaum, J., concurring), *vacated*, 132 S. Ct. 1534 (2012) (mem.).

20. 132 S. Ct. 945 (2012). In the case, the Federal Bureau of Investigation and D.C. Metropolitan Police Department came to suspect a nightclub owner, Antoine Jones, of drug trafficking and used multiple surveillance measures—including visual surveillance and wiretapping—to gather more information. *Id.* at 948. The government also obtained a warrant to attach a GPS device, within ten days of the warrant’s issuance, to Jones’s vehicle while it was in the District of Columbia, but the government attached the GPS after these ten days had elapsed and when Jones’s vehicle was in Maryland rather than the District. *Id.*

21. *See id.* at 957 (Sotomayor, J., concurring) (positing that the Supreme Court should consider revisiting some of the fundamental premises of Fourth Amendment law in light of technological developments); *id.* at 958 (Alito, J., concurring in the judgment) (illustrating that the majority’s reasoning was based on eighteenth century tort law).

22. *Id.* at 955 (Sotomayor, J., concurring) (agreeing with Justice Alito that “longer term GPS monitoring” constitutes a search in most cases).

impinges on expectations of privacy” and should constitute a Fourth Amendment search.²³

The justices did not, however, clearly identify how long or how intense public surveillance must be to cross the constitutional dividing line.²⁴ They did not have to do so because the majority opinion relied on a different rationale to require a warrant. The majority emphasized that the installation of a GPS device on a car prior to tracking was a trespass.²⁵ Because the Supreme Court did not hold that the tracking of public movements alone violated the Fourth Amendment, it did not need to specify the point at which public tracking may violate the Fourth Amendment.²⁶ While this particular instance of public tracking began with a “trespassory” planting of a GPS device,²⁷ other kinds of public surveillance—including most forms of video surveillance—do not. The public street cameras that capture a car’s movements, or those that do so from a drone hovering overhead, do not require police to touch the car—let alone alter it—to surveil its movements.²⁸ When the Justices confront a case like this, they may have to clearly delineate the constitutional boundary line between a search and non-search.

This Article proposes a way to mark that line. It does not do so by asking how long, or how intently, police focus on a particular person or event, but rather by suggesting a different criterion. Whether public surveillance is a search should depend not on duration or the quantity of information gathered by a surveillance method, but rather on that method’s nature or design.²⁹ More specifically, public

23. *Id.* at 964 (Alito, J., concurring in the judgment).

24. *Id.* (noting that “[w]e need not identify with precision the point at which the tracking of this vehicle became a search,” and that while tracking Jones clearly qualified as a search, “[o]ther cases may present more difficult questions”).

25. *Id.* at 949 (majority opinion) (finding that by placing a GPS unit on Jones’s car, “[t]he Government physically occupied private property for the purpose of obtaining information,” which is a clear example of a Fourth Amendment search).

26. *Id.* at 954 (stating that while “[i]t may be that [tracking Jones’s movements] through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, . . . the present case does not require us to answer that question,” and that there was no need to resolve the “vexing problems” regarding how long tracking must be to constitute a search).

27. *Id.* at 949, 952–53 (finding that the government’s planting of the GPS on Jones’s car was a physical intrusion amounting to a trespass and that the “the *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test”).

28. *Id.* at 953–54 (highlighting that visual observation is constitutionally permissible).

29. I previously presented a somewhat different version of this proposal at the 2012 Privacy Law Scholars Conference forum, “From *Jones* to Drones.” See Marc Jonathan Blitz, *United States v. Jones—and the Forms of Surveillance that May Be Left Unregulated in a Free Society*, USVJONES BLOG (June 4, 2012), <http://usvjones.com>

surveillance should count as a search when it takes one of two forms. First, police engage in a Fourth Amendment search, even in public space, when they are not merely observing but also *recording* images or sounds of people. Additionally, the police must obtain these images and sounds from events and people outside the recording officer's presence. In other words, the government does not conduct a search whenever an officer simply turns on an iPhone camera or a camcorder and then records what is happening in front of him. Rather, a public search occurs when recording technology allows officials to record events that they would otherwise not be able to see or hear.³⁰ Second, a search can also occur in public when police magnify and observe details on a person, or the documents or other items she is carrying, so as to reveal information that would not otherwise have been apparent without a pat-down or some other stop-and-search of a person's papers or "effects."³¹

Such a technological form-based or design-based test,³² avoids the key difficulty that plagues an approach that tries, in Justice Alito's words, to exempt "relatively short-term monitoring of a person's movements" from Fourth Amendment restriction, but places constitutional limits on "longer term GPS monitoring" or other surveillance in public.³³ It spares the courts the task of seeking some elusive or arbitrary point in the duration or intensity of a search at which such monitoring morphs from being just another means by which police watch over public space into a possible violation of the Constitution.³⁴ After police begin recording events outside of their

/2012/06/04/united-states-v-jones-and-the-forms-of-surveillance-that-may-be-left-unregulated-in-a-free-society ("[W]hat is important is not the quantity or nature of information actually captured by surveillance, but rather the *nature or form of the surveillance technique itself*").

30. See *infra* notes 116–123 and accompanying text.

31. See *infra* notes 124–129 and accompanying text.

32. Other scholars have also proposed their own distinct versions of such a technological form-based or design-based test for what might count as a search in public. See, e.g., David C. Gray & Danielle Keats Citron, *A Technology-Centered Approach to Quantitative Privacy*, 98 MINN. L. REV. (forthcoming 2013) (manuscript at 5, 25–41), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2129439; Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, ¶¶ 50–70 (setting forth a four-factor test for determining whether new surveillance methods constitute a search) [hereinafter Freiwald, *First Principles*]; Susan Freiwald, *The Four Factor Test*, USVJONES BLOG (June 4, 2012), <http://usvjones.com/2012/06/04/the-four-factor-test> [hereinafter Freiwald, *Four Factor Test*] (questioning what the Fourth Amendment test for GPS tracking should be); see also *infra* Part III.B.2 (discussing these approaches in more detail).

33. *United States v. Jones*, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring in the judgment).

34. See Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 313, 325, 333–34 (2012) (analyzing the difficulties in applying the "mosaic

presence, it does not matter whether they do so for two minutes or two weeks. Police engage in a search simply by using technology with the capacity to create a record of people's movements and aiming it at certain individuals. Defining searches in public spaces in this manner parallels the way that courts typically define Fourth Amendment searches in private spaces. Police are immediately bound by the Fourth Amendment when they enter a person's house, open up and flip through the pages of a diary, or tap a phone line.³⁵ These investigations do not become a search only after they have lasted a certain length of time; rather, the search begins with an entry or intrusion, even if the stay or investigation lasts only seconds or minutes.³⁶ To be sure, the brevity of a search may, in some cases, make it more likely to count as a "reasonable" and permissible search.³⁷ Nevertheless, brevity alone cannot transform such a search into a non-search that is entirely free from Fourth Amendment restriction. The same should be true of public surveillance technologies that involve remote recording or magnification of details normally invisible without a physical search of a person, her documents, or the items she is carrying.

Courts obtain a second advantage by focusing on the nature or design of the investigatory method: The proposed test avoids transforming all police monitoring into a constitutional matter. As Justice Harlan wrote in a 1971 dissent, there is a constitutionally significant difference between monitoring and recording.³⁸ When the government audio records someone's words, it does something

theory," which is a Fourth Amendment approach under which investigatory actions that do not count as a search in isolation count as a search when aggregated).

35. See, e.g., *Kyllo v. United States*, 533 U.S. 27, 37 (2001) ("[T]here is certainly no exception to the warrant requirement for the officer who barely cracks open the front door and sees nothing but the non-intimate rug on the vestibule floor."); *Payton v. New York*, 445 U.S. 573, 590 (1980) (stating that, except in exigent circumstances, the Fourth Amendment requires police to obtain a warrant as soon as they cross the "line" that marks the entrance to the house).

36. See *United States v. Place*, 462 U.S. 696, 706 (1983) (stating that searches, no matter how brief, must be based on probable cause).

37. See, e.g., *Terry v. Ohio*, 392 U.S. 1, 24–25 (1968) (holding that police stop-and-frisk searches, while entailing a search and seizure, require only "reasonable suspicion" and not a warrant or probable cause partly because they, unlike arrests, constitute "a brief, though far from inconsiderable, intrusion").

38. See *United States v. White*, 401 U.S. 745, 785–86 (Harlan, J., dissenting) (asserting that the plurality ignored the differences between third-party monitoring and recording); see also Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 Miss. L.J. 213, 270 (2002) (taking note, but expressing doubt, that the Supreme Court would accept the argument that although "we assume the risk that others will view our public conduct, we do not assume the risk that our public actions will be reduced to a photograph or film").

far more invasive than simply listening to them.³⁹ It creates a record that not only is “free of the possibility of error and oversight that inheres in human reporting,” but also allows officials to review a person’s life in far more detail than they could if they relied only on the fading memories of listeners.⁴⁰

The lesson of Harlan’s contrast is not that recording requires constitutional oversight simply because it reduces our privacy to a greater extent than mere listening or watching. Rather, it is that recording changes the nature of police surveillance in such a way that it threatens privacy as well as other Fourth Amendment interests more deeply. Consider video recording. Such recording does not necessarily reduce an individual’s privacy at the time it occurs: if no one watches the video footage, as it is recorded or afterwards, then the actions captured in the tape remain just as private as they would be had no one seen or captured them.⁴¹ If an officer does watch the scenes captured by the cameras, then an individual’s privacy is compromised to some extent—but the fact that recording is occurring does not make that officer’s live observation any more intrusive than it would otherwise be.

Even unmanned recording, however, raises a significant threat to Fourth Amendment purposes. It takes ephemeral occurrences in our lives and transforms them into permanent records. Through recording technology of this sort, the government can scan its collection of footage of any person’s minute-to-minute activities in hopes of finding something incriminating. Recording, in other words, potentially allows the government to trawl through digital images and audio records in search of evidence that justifies subjecting individuals to state power. Such probing is precisely the kind of dragnet-style investigation that the Fourth Amendment is supposed to restrict⁴²—and does restrict at roadblocks and airports.

39. Cf. *White*, 401 U.S. at 787 (Harlan, J., dissenting) (elaborating that third-party bugging “undermine[s] th[e] confidence and sense of security in dealing with one another that is characteristic of individual relationships between citizens in a free society”).

40. See *id.* at 787–89 (indicating that allowing government officials to monitor private conversations through a willing third-party assistant would compromise the unhindered discourse “that liberates daily life”).

41. See Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393 1418 (2001) (“Being observed by an insect on the wall is not invasive for privacy; rather, privacy is threatened by being subject to *human* observation, which involves judgments that can affect one’s life and reputation.”).

42. See *United States v. U.S. Dist. Court*, 407 U.S. 297, 327 (1972) (Douglas, J., concurring) (stating that “dragnet techniques” are at the heart of the Fourth Amendment’s prohibition on invasive searches).

At such checkpoints, police have limited authority to make suspicionless stops (and searches) to assure safety in these transportation channels. What they may not do under the Fourth Amendment is search for other evidence of crime that such a chokepoint is able to strain out.⁴³ But a dragnet that catches thousands of travelers or other citizens is not the only kind of sweeping investigatory technique that offends Fourth Amendment purposes. For example, dragnet investigations under which officers rummage through possessions or drawers of documents without justification also offend these purposes, even when the hunt for unknown contraband occurs within a single home and focuses on the property of a single homeowner.⁴⁴ A government “fishing expedition” should likewise be deemed to be subject to Fourth Amendment constraints when the data that officials sift through comes not from personal documents, but from the trail of data people leave behind in a world in which every action or movement is recorded for potential review at a later date.⁴⁵

To be sure, public surveillance can threaten Fourth Amendment purposes, even when police are not recording what they see. Police can use telescopes or extremely powerful zoom lenses to scrutinize details on a person’s clothing, or on items or documents removed from a wallet or briefcase, that would be invisible even to bystanders just a few yards away.⁴⁶ Certain courts have suggested that such telescopic magnification would constitute a Fourth Amendment search when pointed at the windows of a home,⁴⁷ and if that is true, it is certainly possible that telescope-aided scrutiny should also be a

43. See, e.g., *City of Indianapolis v. Edmond*, 531 U.S. 32, 40–42 (2000) (striking down as unconstitutional a road block program under which police investigated each car not only for drunk drivers but also for evidence of drug-related contraband); *United States v. Albarado*, 495 F.2d 799, 805 (2d Cir. 1974) (expressing concern about “the possibility that the purpose of the airport search [to prevent terrorism] may degenerate from the original search for weapons to a general search for contraband”); see also *infra* notes 162–167 and accompanying text.

44. See *Andresen v. Maryland*, 427 U.S. 463, 480 (1976) (recognizing that the Fourth Amendment forbids “general, exploratory rummaging in a person’s belongings” (quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971))).

45. See 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, 1407 (2004) (analogizing “mass video surveillance of law-abiding citizens” to “unrestricted house-to-house searches” that the Fourth Amendment clearly prohibits).

46. See *id.* at 1377.

47. See, e.g., *United States v. Tabor*, 635 F.2d 131, 138–39 (2d Cir. 1980) (“The vice of telescopic viewing into the interior of a home is that it risks observation not only of what the householder should realize might be seen by unenhanced viewing, but also of intimate details of a person’s private life, which he legitimately expects will not be observed either by naked eye or enhanced vision.”).

search when it is aimed at the other subjects of Fourth Amendment protection—namely, an individual’s “person, . . . papers, and effects.”⁴⁸ High magnification of a detail on a person or her property may thus, like recording, bring police observation in public onto Fourth Amendment territory.

That such public surveillance is a Fourth Amendment search does not mean that it will always be a Fourth Amendment violation. A search of a house, person, paper, or effect is prohibited by the Fourth Amendment only when it is “unreasonable.”⁴⁹ Just as police, Federal Bureau of Investigation (FBI) agents, and other law enforcement officials frequently use wiretaps by obtaining a warrant or absent such a warrant when circumstances make a wiretap reasonable,⁵⁰ police should be able to capture and examine video records or to closely magnify details of public action when use of these methods count as reasonable.

Part I of this Article discusses why courts have found the Fourth Amendment analysis of public surveillance to be so challenging and describes how they have thus far met this challenge. Part II offers a new test for determining when public surveillance constitutes a search: the government’s actions require Fourth Amendment scrutiny when it records remote events or uses an analogous method of investigation, or, in certain instances, when it employs magnification or sound amplification in a public space. Other kinds of police surveillance in public generally are not searches, even if they employ sophisticated technology. Part III explains why this approach is preferable to various alternatives that scholars, and judges themselves, have considered as they have struggled with how Fourth Amendment law should apply in public. In the course of doing so, Part III describes why police officers will be able to use video surveillance technology, even without a warrant, so long as the police meet Fourth Amendment reasonableness standards that assure the technology is not used in a way that unnecessarily diminishes individuals’ freedom from state monitoring.

48. U.S. CONST. amend. IV.

49. *See id.*; *Maryland v. Buie*, 494 U.S. 325, 331 (1990).

50. *See, e.g., United States v. Williams*, No. 11-6493, 2013 WL 1759941, at *5–6 (6th Cir. Apr. 25, 2013) (affirming the district court’s ruling that a wiretap was permissible because the government proved it was necessary, and the affidavit in support of the intercept order was based on sufficiently reliable evidence).

I. THE NATURE OF THE PROBLEM AND THE SUPREME COURT'S INITIAL STEPS TOWARD A SOLUTION

A. *The Problem of Public Surveillance*

Whether public video surveillance is a search may seem deceptively simple. Since 1967, the Supreme Court has adopted the rule from Justice Harlan's concurrence in *Katz*, under which the government engages in a Fourth Amendment search any time it intrudes upon an "expectation of privacy . . . that society is prepared to recognize as 'reasonable.'"⁵¹ Members of a free society do not expect to be subject to continuous government surveillance, even as they walk or drive on public pathways. As a result, this kind of surveillance should be subject to constitutional limits. Not only do many Americans share this expectation,⁵² but they also likely view it as reasonable and justified, as was clear in the legislative reaction to law enforcement officials' increasing use of drones. The Florida legislature, for instance, recently enacted a law tightly restricting the use of drone surveillance within the State's borders: the Freedom from Unwanted Surveillance Act.⁵³ Additionally, some U.S. Senators and Congressmen have suggested that federal restrictions might also be justified because, as Senator Chuck Grassley explained, "[t]he thought of government drones buzzing overhead, monitoring the activity of law abiding citizens, runs contrary to the notion of what it means to live in a free society."⁵⁴

But the task of fitting public surveillance into Fourth Amendment jurisprudence is, for a number of reasons, more challenging than simply taking note of these intuitions. First, there is the line-drawing problem that confronted the concurrence-writers in *Jones*.⁵⁵ While it

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

52. See Jim Gold, *Poll: Americans OK with Some Domestic Drones—But Not To Catch Speeders*, NBC NEWS (June 13, 2012, 4:15 PM), http://usnews.nbcnews.com/_news/2012/06/13/12205763-poll-americans-ok-with-some-domestic-drones-but-not-to-catch-speeders?lite (describing polls indicating that Americans support drone use for certain security operations, such as securing the border or for "search and rescue" operations, but that 67% oppose the use of drones to issue speeding tickets, and 64% describe themselves as "somewhat concerned" or "very concerned" about drones' effect on their privacy).

53. See Joe Sutton & Catherine E. Shoichot, *Florida Gov. Rick Scott Signs Law Restricting Drones*, CNN (Apr. 28, 2013, 1:42 PM), <http://www.cnn.com/2013/04/25/us/florida-drone-law/index.html> (describing Florida's Freedom from Unwanted Surveillance Act, which restricts the use of police drones within Florida's borders).

54. Brendan Sasso, *Senators Fear Drones "Buzzing Overhead,"* HILL (Mar. 20, 2013, 3:06 PM), <http://thehill.com/blogs/hillicon-valley/technology/289337-senators-worry-about-domestic-drone-surveillance>.

55. See *supra* notes 21–28 and accompanying text (detailing that the concurrences identified the problem but not a solution).

may seem clear that the continuous, suspicionless video recording by hidden government cameras is at odds with a free society, this is not necessarily true of all cases in which police officers watch a person they deem suspicious,⁵⁶ tail a car for a period of time,⁵⁷ or observe a person with low-powered binoculars.⁵⁸ How then, are we to distinguish between permissible, garden-variety watching, and intensive surveillance that offends constitutional principles?

Such problems in drawing Fourth Amendment boundary lines have recently haunted the efforts of courts to resolve the question of whether (and how) the Fourth Amendment applies to police use of GPS surveillance. As noted above, the Supreme Court concurrences in *Jones* found that location tracking is a search only if it lasts a sufficient amount of time, but did not specify how long is too long.⁵⁹ In the lower court opinion in *Jones*, when the case was known as *United States v. Maynard*,⁶⁰ the U.S. Court of Appeals for the D.C. Circuit tried to provide an answer to this question by comparing GPS tracking's incremental intrusions into a person's privacy to what happens when the government assembles pieces of a person's history as though it were piecing together a jigsaw puzzle or "mosaic."⁶¹ To demonstrate this point, the D.C. Circuit noted that while the fact that a person stops at a gynecologist office at one moment may itself tell an observer very little, when police piece this fact together with another GPS reading showing, for example, that she has also stopped at a baby supply store, they can construct a detailed picture of her daily routine and likely infer something about why she followed the path she did (she is pregnant).⁶² But this mosaic theory approach merely begs the questions it is intended to answer: how detailed a picture is too detailed, and how many data points may police collect before they enter constitutional territory?

56. See, e.g., *Christensen v. Cnty. of Boone*, 483 F.3d 454, 460 (7th Cir. 2007) (per curiam) (finding that a police officer did not conduct a search under the Fourth Amendment when he "followed [individuals] in his squad car as they drove on Boone County roads and sat outside businesses that [they] patronized").

57. See, e.g., *United States v. Garcia*, 474 F.3d 994, 997 (7th Cir. 2007) ("[I]f police follow a car around, or observe its route by means of cameras mounted on lampposts or of satellite imaging as in Google Earth, there is no search.").

58. See Ric Simmons, *Why 2007 is Not Like 1984: A Broader Perspective on Technology's Effect on Privacy and Fourth Amendment Jurisprudence*, 97 I. CRIM. L. & CRIMINOLOGY 531, 550 (2007) ("Presumably a law enforcement agent could use a flashlight or a set of binoculars without needing a warrant . . .").

59. See *supra* notes 22–23 and accompanying text.

60. 615 F.3d 544 (D.C. Cir. 2010), *aff'd in part sub nom.* *United States v. Jones*, 132 S. Ct. 945 (2012).

61. See *id.* at 562.

62. *Id.*

Judges are unlikely to provide consistent answers to these questions. This was evident in the case of *United States v. Cuevas-Perez*,⁶³ in which the U.S. Court of Appeals for the Seventh Circuit attempted to apply the D.C. Circuit's Fourth Amendment analysis without expressly endorsing it.⁶⁴ The majority concluded that *Maynard*'s "mosaic" rule simply did not apply to the facts before it because the police had followed Cuevas-Perez for sixty hours, not for twenty-eight days as in *Maynard*, and had tracked his movements on a "single journey," rather than on multiple trips.⁶⁵ The dissent, by contrast, pointed out that monitoring of the defendant on a "60-hour odyssey across 1,650 miles" is far from the kind of brief trip that might be too insignificant to require Fourth Amendment constraints.⁶⁶

The problem is that no apparent principle explicates whether, or why, sixty hours is short enough to remain free from Fourth Amendment restraints. After all, if the danger raised by ongoing GPS surveillance is that it allows police to "connect the dots" of a person's movements and draw inferences about her private plans, a sixty-hour period is probably sufficient time to draw such a connection and make inferences based on the data gathered.⁶⁷ To take the D.C. Circuit's own example from *Maynard*, a woman's visit to a baby supply store may certainly come within sixty hours of her visit to a gynecologist; thus, observers will hardly need twenty-eight days, or even a week, to learn details about that woman's life that are unlikely to be apparent to others in public space. This uncertainty about how much police can learn in a day, or a week, also provides reason to question the Virginia Supreme Court's conclusion that *Maynard*'s mosaic theory should not apply to GPS tracking that lasts less than a week.⁶⁸ It is not clear that a week-long monitoring period is short enough to avoid the dangers of aggregated information that concerned the D.C. Circuit.⁶⁹

The Fourth Amendment line-drawing challenge courts face in public spaces is, in many ways, analogous to the one that Professor Orin Kerr recently addressed in proposing a Fourth Amendment

63. 640 F.3d 272 (7th Cir. 2011), *vacated*, 132 S. Ct. 1534 (2012) (mem.).

64. *See id.* at 274.

65. *Id.*

66. *Id.* at 293 (Wood, J., dissenting).

67. *See id.* at 292–93.

68. *See Foltz v. Commonwealth*, 698 S.E.2d 281, 291 n.12 (Va. Ct. App. 2010) (holding that there was no search or seizure when the police installed a GPS device on the defendant's work van when it was parked in public and used the GPS to track the van while on public streets), *aff'd*, 732 S.E.2d 4 (Va. 2012).

69. *See id.*

regime for Internet communications.⁷⁰ As Kerr pointed out, the key problem in determining whether Internet surveillance constitutes a search is that the natural marker that generally delineates what constitutes a Fourth Amendment search in physical space—namely, the distinction between an enclosed, private space and an observable, public environment—does not exist on the Internet.⁷¹ “The distinction between government surveillance outside and government surveillance inside,” Kerr writes, “is probably the foundational distinction in Fourth Amendment law” because the government does not need any cause or order to conduct surveillance outside,” but “entering enclosed spaces ordinarily constitutes a search that triggers the Fourth Amendment.”⁷² However, the Internet does not fit nicely into this model because there is no outside/inside division to rely upon. Everything on the Internet is considered to be enclosed and inside.⁷³ Kerr therefore argued that Fourth Amendment law needs a new, functionally equivalent distinction to mark the boundary between searches and non-searches.⁷⁴ He proposed that courts should rely on the distinction between content and non-content in e-mails or other Internet communications.⁷⁵ When investigators intercept and read the contents of a person’s e-mail, for example, they are conducting a Fourth Amendment search and must first obtain a warrant or otherwise show their search is reasonable.⁷⁶ Conversely, when investigators merely want to look at the address information on the e-mail, they are doing the equivalent of looking at the outside of an envelope, not the letter inside, and this monitoring of non-content information is therefore not a Fourth Amendment search.⁷⁷

If Internet surveillance raises a Fourth Amendment problem because everything is “inside,” public surveillance raises a similar problem because everything is outside. Public surveillance is “public” because it focuses on the outside world and, more specifically, on visible behavior in it. Here too, then, Fourth Amendment law needs

70. See generally Kerr, *supra* note 11.

71. *Id.* at 1009–10.

72. *Id.* at 1010.

73. *Id.* at 1012.

74. See *id.* (“The inside/outside distinction no longer serves the basic function in the Internet setting that it serves in the physical world.”).

75. *Id.* at 1007–08.

76. *Id.* at 1020.

77. *Id.* at 1019; see also Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 WM. & MARY L. REV. 2105, 2115–16 (2009) (proposing, based on case law, the existence of a content/non-content distinction between searches and non-searches in Internet communications).

a replacement for the outside/inside distinction. It needs a new boundary line to demarcate parts of the outside world that deserve to be treated like inside spaces for Fourth Amendment purposes—parts of our life in public that, like our living rooms and bedrooms, deserve to be constitutionally insulated from government scrutiny.

The lack of a replacement for the outside-inside distinction in public space leaves judges without a key resource for determining what counts as a search in public space. Without such a line, it is difficult for courts to pronounce long-lasting public surveillance to be a search on the basis that certain forms of it seem disturbingly intrusive.⁷⁸ These intrusions do not, by themselves, tell us how to distinguish investigations that are invasive enough to require constitutional oversight from those that are not.

There is a second difficulty in treating public surveillance as a search: if courts subject police to significant constitutional limits in monitoring public space, they risk crippling law enforcement's efforts to do what it is charged with doing. Police are not only generally as free as other citizens to watch the streets they patrol, they are duty-bound to do so. So it seems counterintuitive to require police to obtain a warrant before showing the vigilance they are required to show as a condition of their work.

One might suggest that courts should impose Fourth Amendment requirements only on focused investigations of public space and not on casual observations that police make while on patrol. But even this approach arguably restricts police too tightly. Because law enforcement is generally barred from conducting warrantless investigations of homes and other private spaces, it needs to begin an investigation somewhere else—in the public space outside of the home. As the Supreme Court noted in *California v. Ciraolo*,⁷⁹ in order to obtain the probable cause required to obtain a warrant, police must begin investigating and collecting evidence before they have probable cause.⁸⁰ Thus, there needs to be *some* place to start.⁸¹ In short, if courts and scholars extend Fourth Amendment protection beyond homes, private drawers, and journals into the realm of public and visible activity, they have to recognize that they are extending it into a realm that is, in many ways, and to a far greater extent than the

78. See *California v. Ciraolo*, 476 U.S. 207, 226 (1986) (Powell, J., dissenting) (recognizing that rapidly advancing technology will continue to alter the method of Fourth Amendment analysis).

79. 476 U.S. 207 (1986).

80. *Id.* at 213.

81. *Id.* (postulating that the chance to make observations from the public space is “precisely what a judicial officer needs to provide a basis for a warrant”).

activity in a home or other private environment, very much the government's business.

Effective investigation, moreover, often requires police to take advantage of new surveillance technologies. As the Seventh Circuit noted in an earlier GPS case, the Fourth Amendment "cannot sensibly be read to mean that police shall be no more efficient in the twenty-first century than they were in the eighteenth."⁸²

B. A Simple, but Flawed, Position: Treating Open Areas as a Fourth Amendment Free Zone

One possible response to such concerns is to err, at least in public spaces, on the side of giving government all of the room it needs to conduct investigations. In short, we might simply adopt the rule that surveillance of what is visible and public never constitutes a search. In applying the Fourth Amendment to public space, in other words, we might conclude that we do not need a substitute for the outside/inside distinction because that dichotomy itself provides a simple and satisfactory answer: everything that is left visible and audible in the outside world is "outside" and therefore may be observed by the government free from constitutional restraint.⁸³

At least on the surface, this is the approach that the Supreme Court has taken to public investigations so far (or at least until its 2012 *Jones* decision).⁸⁴ The Court has allowed the government to track the movements of automobiles with radio transmitters, for example, so long as the tracking occurs "on public thoroughfares" and does not extend inside the home.⁸⁵ It has permitted officials to observe the property of a factory, and even the outskirts of private homes, from planes and helicopters in "public airspace" where the public has a right to be and observe what is around it.⁸⁶ In fact, decades before

82. *United States v. Garcia*, 474 F.3d 994, 998 (7th Cir. 2007).

83. For an argument largely favoring such a position, see Heidi Reamer Anderson, *The Mythical Right to Obscurity: A Pragmatic Defense of No Privacy in Public*, 7 I/S: J.L. & POL'Y FOR INFO. SOC'Y 543 (2012).

84. *See, e.g., Ciraolo*, 476 U.S. at 213 (restating that what an individual knowingly exposes to the public is not protected by the Fourth Amendment).

85. *See, e.g., United States v. Karo*, 468 U.S. 705, 721 (1984) (holding that investigatory actions do not constitute a search when they are observing that which can be seen by the public); *United States v. Knotts*, 460 U.S. 276, 281 (1983) (explaining that traveling over public streets voluntarily conveys information to anyone who might be watching with the naked eye or with the assistance of technology).

86. *See Ciraolo*, 476 U.S. at 212–13 (holding that investigators do not violate the Fourth Amendment when they observe property from public airspace and members of the general public flying overhead could make the same observation); *Dow Chem. Co. v. United States*, 476 U.S. 227, 239 (1986) (finding that the Environmental Protection Agency's fly-by assessment of an industrial complex to observe whether it

radio transmitters and chartered planes became a common feature of everyday life, the Supreme Court—in a 1924 decision written by Justice Holmes—made clear that “the special protection accorded by the Fourth Amendment to the people in their ‘persons, houses, papers and effects’ is not extended to the open fields.”⁸⁷ The “open fields” doctrine later seemed to some to be at odds with the Court’s holding in *Katz*, in which the majority held that electronic eavesdropping is a Fourth Amendment search even when it targets someone making a call from a public phone booth on a street.⁸⁸ The *Katz* majority had called into question the notion that everything we do in public may be monitored free of constitutional restraint, declaring that what a person “seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.”⁸⁹

But the Supreme Court later made clear that the open fields doctrine remains a central part of the Fourth Amendment law. In *Oliver v. United States*,⁹⁰ the Court squarely rejected a property owner’s claim that the police had violated the Fourth Amendment when they located a marijuana field on his land.⁹¹ Unlike a realm where individuals might reasonably expect privacy, said the Court, “open fields do not provide the setting for those intimate activities that the Amendment is intended to shelter from government interference or surveillance.”⁹² Courts have understood this “open fields” doctrine to mean that police are free to observe not only what is visible in a field, but also what they can see in public streets and roads.⁹³

Such an approach still leaves individuals with an opportunity to find sanctuaries for privacy in public space, but only when they find pockets of “inside” space somewhere in the public, visible world. People might, for example, hide items they bring onto a street within a purse or briefcase. They might keep confidential conversations secret by engaging in them only from a closed phone booth⁹⁴ or from

was in compliance with environmental regulations did not constitute a Fourth Amendment search).

87. *Hester v. United States*, 265 U.S. 57, 59 (1924).

88. *Katz v. United States*, 389 U.S. 347, 353 (1967); see also, Bruce G. Berner, *The Supreme Court and the Fall of the Fourth Amendment*, 25 VAL. U. L. REV. 383, 390 (1991) (recalling that many commentators predicted that *Hester*’s open-field doctrine would no longer be applicable after *Katz*).

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

90. 466 U.S. 170 (1984).

91. See *id.* at 173, 182–84.

92. *Id.* at 179.

93. See, e.g., *California v. Ciraolo*, 476 U.S. 207, 213–15 (1986).

94. See, e.g., *Katz*, 389 U.S. at 353 (finding the government engaged in a search when its eavesdropping invaded “the privacy upon which [the defendant] justifiably relied while using the telephone booth”).

behind the locked doors and closed windows of an automobile.⁹⁵ It was this kind of privacy in public that the Supreme Court endorsed and protected in *Delaware v. Prouse*⁹⁶ when it emphasized that “people are not shorn of all Fourth Amendment protection when they step from their homes onto the public sidewalks” or when “they step from the sidewalks into their automobiles.”⁹⁷ Even on public streets, drivers remain protected from having their cars arbitrarily stopped and searched,⁹⁸ and pedestrians are protected from being stopped and frisked for weapons unless an officer has “reasonable” suspicion that they are involved in criminal activity.⁹⁹ But these types of Fourth Amendment protections only shield what is inside of one’s car or inside of one’s pockets. They do not limit a police officer’s freedom to observe the outside of the car or its movements, or to scrutinize the outside of a person’s jacket.¹⁰⁰

There are a number of advantages to this bright-line rule that denies Fourth Amendment protections to observations that are visible to the public. One is that it keeps Fourth Amendment law consistent with the classic principle of search and seizure law, enunciated in the 1765 case of *Entick v. Carrington*,¹⁰¹ that “the eye cannot . . . be guilty of a trespass.”¹⁰² While this English case antedated the enactment of the U.S. Bill of Rights in 1791, it was familiar to the Framers and was an important inspiration, and source for, Fourth Amendment jurisprudence.¹⁰³ Its assumption that officials do not commit an unreasonable search simply by looking at what they can see has become a key principle in that jurisprudence.¹⁰⁴

95. See, e.g., *Delaware v. Prouse*, 440 U.S. 648, 658–59, 663 (1979) (holding that stopping an automobile and requesting the driver’s license and registration involves a search and is only permissible under the Fourth Amendment where there is reasonable, articulable suspicion to do so).

96. 440 U.S. 648 (1979).

97. *Id.* at 663.

98. See *id.* (requiring that officers may only stop and detain motorists if “there is at least articulable and reasonable suspicion” that the motorist has violated the law).

99. See *Terry v. Ohio*, 392 U.S. 1, 19, 24–25 (1968) (highlighting the need to grant officers a means of determining whether a person poses a threat of physical harm and a way to neutralize that risk).

100. See generally *United States v. Jones*, 132 S. Ct. 945, 953 (2012) (“This Court has to date not deviated from the understanding that mere visual observation does not constitute a search.”).

101. 19 Howell’s State Trials 1029 (C.P. 1765).

102. *Id.*, in 19 Howell’s State Trials 1029, 1066 (C.P. 1765).

103. See *Boyd v. United States*, 116 U.S. 616, 626–27 (1886) (explaining that, during the Revolutionary Period, American statesmen were familiar with *Entick*, the “monument of English freedom,” and its propositions were unquestionably in the minds of the Framers as they created the Fourth Amendment).

104. See, e.g., *California v. Ciraolo*, 476 U.S. 207, 213–15 (1986) (holding that police do not violate the Fourth Amendment when they observe what is visible to the public).

As Justice Scalia noted in *Jones*, “This Court has to date not deviated from the understanding that mere visual observation does not constitute a search.”¹⁰⁵

When police search inside of a home or another private environment, of course, they engage in more than mere observation. They first enter the space, thereby transforming their subsequent observations into a search requiring a warrant (or some other showing of constitutional reasonableness).¹⁰⁶ By contrast, in public spaces, police can often observe an individual’s movements and other activities without having to set foot on anyone else’s property.¹⁰⁷ To the extent they invade the privacy of the person they watch, they often do so simply through observing.

A second advantage of denying Fourth Amendment protections to observations of what is visible in public is its simplicity and clarity. It draws a clear line for police officers and citizens. What is inside a home or office is protected; what is outside in public space is not. To be sure, this kind of simple division does not line up perfectly with individuals’ expectations of privacy. Individuals may well be more eager to hide certain activities they conduct in public life, such as travelling to a psychotherapist’s office or visiting an X-rated movie theater, than they are to hide many mundane activities in their home life, such as their choice of what to have for breakfast. But perhaps it is not plausible to calibrate Fourth Amendment protections to the privacy that individuals expect in each discrete activity.

The Supreme Court has certainly not tried to adjust the degree of protection on an activity-by-activity basis in applying the Fourth Amendment to in-home activity. On the contrary, as the Court emphasized in *Kyllo v. United States*,¹⁰⁸ “[i]n the home, . . . all details are intimate details, because the entire area is held safe from prying government eyes.”¹⁰⁹ It therefore does not matter that the activities the government observes in gathering information from a home are not particularly embarrassing or sensitive.

The Fourth Amendment errs on the side of protecting the privacy of all in-home activity; perhaps it should err in the other direction outside the home. If the public needs some protected space where it can count on privacy without worrying about whether a particular activity is or is not sufficiently intimate to be shielded, government

105. *Jones*, 132 S. Ct. at 953.

106. *See id.* at 954–55 (Sotomayor, J., concurring).

107. *See id.* at 949–50 (majority opinion).

108. 533 U.S. 27 (2001).

109. *Id.* at 37 (holding that the use of thermal imagers to detect the heat emissions coming from a house is a search under the Fourth Amendment).

officials might also need some space where they can watch potentially illegal activities without worrying, during each observation, whether the activity they are watching is too private to look at (for too long) without a warrant.¹¹⁰ Such a bright-line rule arguably would not only provide certainty for police, but also reassure the population that relies on them that law enforcement will be able to act proactively and effectively to investigate and thwart criminal activity.

It is perhaps therefore not surprising that while the D.C. Circuit in *Maynard* ventured to extend Fourth Amendment limits to public surveillance,¹¹¹ the other circuits to address the issue have found that GPS tracking is a non-search by virtue of the fact that the information it collects comes solely from a driver's public and observable activity.¹¹² The Seventh Circuit, for example, noted in 2007 that while GPS surveillance may threaten our privacy, it does not do so in a way that makes it a Fourth Amendment search.¹¹³ Rather, it is a high-tech analogue for visual tracking of a kind police have long done free from constitutional restriction.¹¹⁴ "[I]f police follow a car around, or observe its route by means of cameras mounted on lampposts or of satellite imaging as in Google Earth, there is no search," and when police "follow" the same car with GPS tracking technology, they are "on the same side" of this constitutional "divide."¹¹⁵ The Seventh Circuit reaffirmed this position on GPS tracking after *Maynard* was decided, noting again that so long as GPS tracking is limited to public space, it reveals no more than what is already visible.¹¹⁶ The Eighth

110. Arguably, this clear division of inside "protected areas" and outside unprotected ones is at odds with the Court's oft-repeated language in *Katz* that "[t]he Fourth Amendment protects people not places," and the key question is therefore not about where a person is, but what that person reasonably expects will remain private from the government. *Katz v. United States*, 389 U.S. 347, 350, 351–52 (1967) (holding that "[w]hat a person knowingly exposes to the public, even in his own home or office," is unprotected, and "what he seeks to preserve as private, even in an area accessible to the public," is constitutionally shielded). But the inconsistency may be only superficial. If we preserve privacy in public by enclosing our property or action inside of a hidden space, and we expose our action in the home by leaving it visible to people on the street, then *Katz* still tracks the outside/inside distinction quite well. We lose our privacy inside the home when we leave an in-home action visible to those in the outside world, and we can gain a measure of privacy in public by finding a way to shroud it inside some kind of enclosed container or other space.

111. *Maynard v. United States*, 615 F.3d 544, 556 (D.C. Cir. 2010), *aff'd in part sub nom. Jones*, 132 S. Ct. 945.

112. *See, e.g.*, *United States v. Marquez*, 605 F.3d 604, 609–10 (8th Cir. 2010); *United States v. Pineda-Moreno*, 591 F.3d 1212, 1216 (9th Cir. 2010), *vacated*, 132 S. Ct. 1533 (2012) (mem.); *United States v. Garcia*, 474 F.3d 994, 997 (7th Cir. 2007).

113. *Garcia*, 474 F.3d at 998.

114. *Id.*

115. *Id.* at 997.

116. *Id.* at 997–98.

and Ninth Circuits likewise applied Supreme Court precedent to conclude that police no more engage in a Fourth Amendment search when they track a car in public space using GPS technology than when they track a car by following it.¹¹⁷ Video surveillance would, for example, not only show that a particular car parked near a doctor's office, but also that a particular person emerged from the car, went inside the office, and perhaps came out carrying a worried look on her face. It would indicate not only that a person parked near a particular bookstore or DVD store, but also, perhaps, what book or movie she carried out of the store.¹¹⁸ These activities, of course, take place in public where a person might be seen by others nearby, including police officers. But in a world without ubiquitous public surveillance, others are unlikely to focus on, let alone remember, activities of strangers that have no significance to them. A video archive, by contrast, gives interested officials a way to scrutinize (and review) such acts after the fact, even if they have no probable cause or other reasonable basis to track them.¹¹⁹ In short, if public and visible space remains a Fourth Amendment-free zone, it provides room not only for police to vigilantly watch the streets (as we expect them to do), or perhaps notice and scrutinize activities that seem suspicious, it also provides them with unlimited space to record, track, and review the minute-by-minute activities of individuals they have no reason to suspect of a crime. This includes activities that, although occurring in public, deal with medical issues, reading preferences, or other traditionally private information.¹²⁰

117. See, e.g., *Marquez*, 605 F.3d at 609–10 (stating that no search occurs when the use of GPS technology does not infringe upon a person's privacy); *Pineda-Moreno*, 591 F.3d at 1216 (explaining that GPS technology serves as a substitute for physically following a car on public roads and therefore similarly does not constitute a Fourth Amendment search).

118. See generally Adam Schwartz, *Chicago's Video Surveillance Cameras: A Pervasive and Poorly Regulated Threat to Our Privacy*, 11 NW. J. TECH. & INTELL. PROP. 47, 23 (2013) ("Without proper regulation, each of us must wonder whether the government is watching and recording us when we walk into a book store, a political meeting, or a psychiatrist's office.").

119. See Blitz, *supra* note 45, at 1356 (describing how a video archive can allow the government to virtually "randomly stop and closely scrutinize numerous people," exactly the type of searches the Fourth Amendment prevents).

120. See *United States v. Jones*, 132 S. Ct. 945, 955 (2012) (listing examples of public movements that could reveal private details (citing *People v. Weaver*, 909 N.E.2d 1195, 1199 (N.Y. 2009))).

*C. The Supreme Court's Signals About Fourth Amendment
Protection in Public Spaces*

Perhaps because it was aware that there is sometimes a need for privacy protection in public, the Supreme Court, even before its 2012 *Jones* decision, occasionally gave signals in dicta that it might carve out some exceptions to its bright-line rule that what is public and observable is not constitutionally protected from observation.¹²¹ It pointed specifically to two kinds of potential exceptions: (1) circumstances in which magnification of what is visible from public airspace may reveal, not merely the contents of a field or greenhouse or the design and operation of a factory, but internal “intimate activity”;¹²² and (2) circumstances in which public surveillance is not simply targeted at a particular person for a discrete time period, but rather constitutes “dragnet” or “round-the-clock” tracking of a person’s activities.¹²³

Consider first some of the worries that the Court has raised about magnification. In all three of the aerial surveillance cases that the Court has heard, it held that aerial surveillance of a home’s curtilage, or the property outside a factory, from a plane or helicopter did not count as a search subject to Fourth Amendment protection.¹²⁴ Instead, the Supreme Court stated that it *might have* been a protected search had high-powered magnification technology allowed government officials to observe not simply the property below, but intimate activity or perhaps personal property located on it that revealed elements of a person’s past or personality.¹²⁵ In *Dow Chemical Co. v. United States*,¹²⁶ the Court held that Environmental Protection Agency officials did not trigger Fourth Amendment limits when they photographed details of a factory they suspected of pollution with a powerful map-making camera.¹²⁷ But, as the Court emphasized in a footnote, this was not a case where the government’s

121. See, e.g., *Dow Chem. Co. v. United States*, 476 U.S. 227, 238 (1986) (noting that using satellite surveillance technology might require a warrant in order to be constitutional).

122. See *infra* notes 124–134 and accompanying text (reviewing the Court’s discussions of potential constitutional issues with magnification).

123. See *infra* notes 135–138 and accompanying text (reviewing the Court’s cases related to tracking devices).

124. *Florida v. Riley*, 488 U.S. 445, 449–50 (1989) (plurality opinion) (curtilage of a home); *Dow Chem. Co.*, 476 U.S. at 239 (industrial complex); *California v. Ciraolo*, 476 U.S. 207, 213 (1986) (curtilage of a home).

125. See *Dow Chem. Co.*, 476 U.S. at 238 (explaining that the magnification at issue in the case was not strong enough to expose “intimate details,” which would raise constitutional concerns).

126. 476 U.S. 227 (1986).

127. *Id.* at 239.

magnification revealed small items such as a “class ring” or “identifiable human faces or secret documents captured in such a fashion as to implicate more serious privacy concerns.”¹²⁸ Similarly, in *Ciraolo*, which was decided on the same day as *Dow Chemical Co.*, the Court hinted at the same “intimate details” protection against public surveillance.¹²⁹ It held that police did not violate reasonable expectations of privacy when they used a fly-over airplane to observe marijuana in the defendant’s backyard.¹³⁰ But it also stressed that the State itself had acknowledged that some fly-over observation might well be a search when it employs “modern technology” to reveal “those intimate associations, objects or activities otherwise imperceptible to police or fellow citizens.”¹³¹ And it included the same hint in *Florida v. Riley*,¹³² even as it refused to find the police engaged in a Fourth Amendment search when they hovered over the defendant’s greenhouse in a helicopter and peered through a crack in its roof to verify that it contained marijuana plants.¹³³ The Court made clear that there was no evidence that the state’s aerial observation revealed any “intimate details connected with the use of the home or curtilage.”¹³⁴ In short, where the state uses magnification to reveal intimate details in a home’s curtilage, it may well be engaged in a search—even if those details are visible from public airspace. The same might be true of magnification that is aimed, not at a home’s curtilage, as in *Ciraolo* and *Riley*, or a business’s property, as in *Dow Chemical Co.*, but at activities in streets, parks or open fields.

The Supreme Court also suggested, even before the concurrences in *Jones*, that ongoing location tracking may reveal hidden details and thus become a search. In its 1983 *Knotts* decision, the Court held that police do not engage in a search when they use a radio transmitter to track a driver’s movements on public roadways, while acknowledging that more invasive location tracking might be a protected search.¹³⁵ The Court noted the concern that finding the police conduct at issue

128. *Id.* at 238 n.5.

129. *See Ciraolo*, 476 U.S. at 215 & n.3 (noting that the use of technology to aid the naked eye might change Fourth Amendment analysis).

130. *Id.* at 215.

131. *Id.* at 215 n.3.

132. 488 U.S. 445 (1989).

133. *See id.* at 450–51 (plurality opinion) (explaining why an expectation of privacy from the air was unreasonable).

134. *Id.* at 452.

135. *See United States v. Knotts*, 460 U.S. 276, 284 (1983) (discussing the Eighth Circuit’s finding that “intrusive” surveillance could be prohibited by the Fourth Amendment but noting the limited invasiveness of the search used in this case).

in *Knotts* to be within constitutional limits would mean that police would likewise be free of all constitutional restraint if they conducted “twenty-four hour surveillance of any citizen” on a whim.¹³⁶ Such a “dragnet-type law enforcement practice[,]” suggested the Supreme Court, might be subject to Fourth Amendment limits, even if limited location tracking with a radio transmitter is not.¹³⁷ In *Maynard*, the D.C. Circuit seized upon this reasoning and held that a twenty-eight day period of continuous GPS surveillance was precisely the kind of ongoing surveillance that the Court in *Knotts* explained would be constitutionally problematic.¹³⁸

Taken by themselves, these dicta do not provide ready-to-apply Fourth Amendment rules for identifying searches in public spaces. First, they do not provide the kind of identifiable boundary line between searches and non-searches that law enforcement officers need in order to know whether a particular search technique requires a warrant. As noted earlier, there is no guiding principle for when location tracking or video surveillance has occurred for too long of a period—or collected too much information—to remain free of constitutional limits.¹³⁹ The same problem arises for a rule that constitutionally shields “intimate” activities from magnification technologies but leaves other types of activities, such as movements on a road, free-for-the-taking. While certain activities, such as those involving family interactions, romantic relationships, or medical appointments, may intuitively be inappropriate for a state official to spy upon, the fact is that people are different. What may be personal and private for one person may not be for another. People are idiosyncratic, and what is truly private is a matter of social context.¹⁴⁰ For example, if a person is seeking a new job, he may want to buy books on switching careers or visit a resume workshop without his employer discovering these actions. These kinds of activities may not be all that private for other people, such as a college student who, like many others about to graduate, has to prepare herself for the job market. But, those actions may be private for a long-time employee who wants to, and perhaps must, hide his plans for a career-change from a current boss. Courts are ill-equipped to make these distinctions. Unlike a line that divides all content-based information

136. See *id.* at 283–84 (deferring constitutional analysis of such practices).

137. *Id.* at 284.

138. *United States v. Maynard*, 615 F.3d 544, 556–57 (D.C. Cir. 2010), *aff’d in part sub nom.* *United States v. Jones*, 132 S. Ct. 945 (2012).

139. See *supra* text accompanying notes 22–24.

140. See Blitz, *supra* note 45, at 1412 (giving examples of situational and individual factors that can influence the level of privacy desired).

in an e-mail from non-content based information, such as an e-mail address, a line that divides some kinds of “intimate” content from other kinds of content is a hard line for courts to mark.

Still, the Supreme Court’s dicta about magnification and location provides a foundation to build upon. The suggestion in its aerial surveillance cases—that some types of magnification would count as a search—captures a widely shared intuition; namely, that even in public space, we may desire, and should still be able, to keep certain details of our lives from being seen by others with whom we share that space. Even in the outside world, certain details of our activity may be so difficult for others to notice that they are akin to details we have enclosed in a bag or a car. These activities are essentially invisible because of their small size, the distance, or the limits of natural human vision and human attention. These factors can hide them almost as effectively as the invisibility created by a wall or enclosure that blocks light. Details that cannot typically be seen without magnification, because of size, distance, or visual limitations, might constitute one category of outside information that should be treated as “inside” for Fourth Amendment purposes.

The same is arguably true of information about us that can be obtained only by aggregating numerous public observations of our activity taken from a wide swathe of public space. This is the argument at the heart of the mosaic theory that the D.C. Circuit used in *Maynard* to find that GPS surveillance was a search.¹⁴¹ The D.C. Circuit held:

[T]he information the police discovered in this case—the totality of Jones’s movements over the course of a month—was not exposed to the public: . . . unlike one’s movements during a single journey, the whole of one’s movements over the course of a month is not *actually* exposed to the public because the likelihood anyone will observe all those movements is effectively nil.¹⁴²

Just as magnification reveals information that is effectively invisible to observers in public space, so too did GPS surveillance in this case. This information therefore also might be deemed to be akin to “inside” information, which is generally not available to individuals who make only surface-level observations of the activity around them and do not deepen their observations with the aid of sophisticated technology or a large coordinated team of observers.

141. See *Maynard*, 615 F.3d at 562 (discussing the government’s use of the mosaic theory to justify collecting information for national security purposes).

142. *Id.* at 558.

Yet, while the Supreme Court has been right to express concerns about certain kinds of magnification and about location tracking and right not to make every instance of magnification and location tracking a Fourth Amendment concern, it may have created future challenges by suggesting that the way to distinguish worrisome from unproblematic uses of these technologies requires courts to look at the amount or type of information gleaned. As discussed in the next Part, courts can better build upon the Supreme Court's concerns by focusing on the type or design of technology that the government uses to magnify details or record a person's path through public space.

II. ANOTHER SOLUTION: RECORDING AND MAGNIFICATION SEARCHES

A. *Constitutionalizing Public Surveillance: The Proposed Test*

This Part proposes another way to mark the line between searches and non-searches in public space. The core element of this proposal is to treat all police recording of public movements and activities that occur outside the presence of the officer doing the recording as a Fourth Amendment search. In short, the government engages in a search not merely when it watches a person, but when it systematically collects information about her by recording what she does. In the absence of a recording, magnification of the items a person is carrying should likewise count as a "search" if the magnification reveals details about "persons, houses, papers, persons, [or] effects" that would only be discovered in a more traditional search. This would require courts to be able to clearly identify situations where magnification has the same effect as traditional searches, such as a home entry, a pat down, or the unauthorized interception and review of mailed or e-mailed documents.

This proposed test addresses the line-drawing problem because, under this approach, it does not matter how long police investigate a person's public activities, but rather what technology they use to investigate the individual. If the police use technology that can capture images or record video or locations of individuals outside the presence of the police officer doing the recording, then the investigation counts as a search from the moment the officer hits the "record" button. Even if the recording lasts only a minute, it is a search. After all, a wiretap or use of an electronic "bug" would count as a search from the moment it begins giving police access to the conversation on which they are eavesdropping. The same would be true of recording-free tracking and magnification-aided investigations

described above. Once courts assure themselves that police are using this advanced technology, any resulting investigation would be classified as a “search,” regardless of its duration or detail.

Nor would such searches involve “mere visual surveillance.” While the “eye cannot . . . be guilty of” Fourth Amendment violations,¹⁴³ electronic monitoring of otherwise inaccessible data can be unconstitutional. Such electronic monitoring, for example, often counts as a “search” when it is used to intercept conversations.¹⁴⁴ It should likewise count as a search when it is used to record individuals’ movements and activities in public space.

Another reason to focus on the recording of remote activities as a trigger for Fourth Amendment protection is based on the fact that courts and scholars alike often identify the central purpose of the Fourth Amendment as protecting privacy. For example, Professor Sherry Colb, a Fourth Amendment expert, made this claim in responding to the notion that the Fourth Amendment only protects privacy in a limited way—by protecting the privacy we receive from control we exercise over our homes, cars, or other property.¹⁴⁵ The Framers’ goal in the Fourth Amendment, she wrote, can be best understood as protecting “privacy in all of its incarnations.”¹⁴⁶ Such an emphasis on privacy is understandable given the Supreme Court’s interpretation of the Fourth Amendment since 1967. Under the definition of “search” the Court has used since *Katz*, Fourth Amendment protections are triggered only when government invades “a reasonable expectation of privacy.”¹⁴⁷ As a result, judges and commentators often have understandably assumed that it is precisely such an expectation of privacy, whether tightly linked to property or

143. *Kyllo v. United States*, 533 U.S. 27, 32 (2001) (quoting *Boyd v. United States*, 116 U.S. 616, 628 (1886)).

144. See, e.g., *United States v. U.S. Dist. Court*, 407 U.S. 297, 313 (1972) (“[B]road and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate the application of Fourth Amendment safeguards.” (footnote omitted)).

145. See generally Sherry F. Colb, *A World Without Privacy: Why Property Does Not Define the Limits of the Right Against Unreasonable Searches and Seizures*, 102 MICH. L. REV. 889, 895–96 (2004) (discussing the privacy issues related to a hypothetical mindreading device).

146. *Id.*

147. See *Katz v. United States*, 389 U.S. 347, 360 (1967) (Harlan, J., concurring); see, e.g., *United States v. Jones*, 132 S. Ct. 945, 950 (2012) (“Our later cases have applied the analysis of Justice Harlan’s concurrence in [*Katz*], which said that a violation occurs when government officers violate a person’s reasonable expectation of privacy” (internal quotation marks omitted)); *Kyllo*, 533 U.S. at 33 (describing multiple Supreme Court cases applying the test from “Justice Harlan’s oft-quoted concurrence,” under which “a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable”).

not, that the Fourth Amendment is intended to protect.¹⁴⁸ Thus, Justice Alito's concurrence in *Jones* focused on understanding whether the GPS tracking in that case intrudes upon a "constitutionally protected sphere of privacy."¹⁴⁹ Even critics of the *Katz* test, such as Professor Anthony Amsterdam, have spoken in similar terms about Fourth Amendment purposes, arguing that its core function is to prevent government attacks on privacy and freedom that would be "inconsistent with the aims of a free and open society."¹⁵⁰

But as the *Katz* majority itself observed, "privacy" is too general a description of what the Fourth Amendment protects.¹⁵¹ "The Fourth Amendment," it observed, "cannot be translated into a general constitutional 'right to privacy.'"¹⁵² Rather, it protects privacy against "certain kinds of governmental intrusion."¹⁵³ The challenge facing courts then is to pinpoint which types of governmental invasions into privacy implicate Fourth Amendment purposes and which do not. This is an important question for courts to ask as they analyze public surveillance. After all, every time a police officer stares at a person who is standing on the street or driving on the road, that officer is, in some small measure, lessening that person's privacy vis-à-vis the state. He is watching activity that might otherwise go unnoticed by any representative of the state. The same is true if an officer at a police center watches a monitor displaying images from a remote street camera. These are invasions of privacy, but that alone does not make them violations of the Fourth Amendment. Rather, courts must also assess whether the state's reduction in our privacy in these cases is accomplished by the "kinds of governmental intrusion" that the Fourth Amendment prohibits.¹⁵⁴

Unfortunately, the test that courts rely on most heavily to address this challenge—the reasonable expectations of privacy test—sounds precisely like a test for implementing the general right of privacy that

148. See, e.g., *United States v. Maynard*, 615 F.3d 544, 555–65 (D.C. Cir. 2010) (exploring whether the use of a GPS device violated the defendant's "reasonable expectation of privacy"), *aff'd in part sub nom. Jones*, 132 S. Ct. 945.

149. *Jones*, 132 S. Ct. at 964 (Alito, J., concurring in the judgment).

150. Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 403 (1974).

151. See *Katz*, 389 U.S. at 350 (explaining that while the Fourth Amendment protects privacy, "its protections go further, and often have nothing to do with privacy").

152. *Id.*

153. See *id.* at 350 & n.4. (emphasis added) (discussing seizures of person and property as also being protected by the Fourth Amendment whether they occur in public or in private).

154. See *id.* at 350.

the *Katz* majority had sought to distinguish from the Fourth Amendment right against unreasonable searches. Rather than limit Fourth Amendment safeguards to certain government intrusions into privacy, that test subjects *all such* intrusions that interfere with the privacy that individuals reasonably rely upon to constitutional limits.

Judges have sometimes emphasized that the requirement for reasonable reliance is itself a limit.¹⁵⁵ Even if a person expects privacy on a public street (satisfying the first prong of the reasonable expectations test), such an expectation is not one society is prepared to recognize as reasonable (failing the second prong).¹⁵⁶ But this limit is not all that helpful. First, the privacy we reasonably rely upon can be easily diminished, as Professor Amsterdam has highlighted, and the Supreme Court soon after acknowledged, by government action itself.¹⁵⁷ By putting people on notice that they will be subject to GPS monitoring, for example, the government could make it unreasonable to expect freedom from such monitoring. Moreover, the test also seems to place Fourth Amendment law on quickly shifting sands. An expectation of privacy can change quite rapidly as technology advances, and social norms change from year to year.¹⁵⁸ Perhaps for this reason, the Supreme Court has often interpreted “reasonable expectation of privacy” in a way that seems at odds with common intuitions about when citizens can expect privacy and, as Professors Christopher Slobogin and Joseph Schumacher have shown, with empirical data about such expectations.¹⁵⁹

Still, there is reason to take seriously—and try to better elaborate upon—the Supreme Court’s statement in *Katz* that the Fourth Amendment protection against unreasonable searches is narrower than a general “right of privacy.” As the legal scholar William Stuntz

155. See, e.g., *Florida v. Riley*, 488 U.S. 445, 450–51 (1989) (plurality opinion) (focusing on the fact that the defendant had a reasonable expectation of privacy from ground-level observation, but not from aerial observation).

156. Cf. *id.* at 452, 454 (O’Connor, J., concurring) (arguing that the plurality erred by focusing on the helicopter being in legal airspace, when the real test was whether the helicopter was in airspace used “with sufficient regularity” that its presence would be reasonable to society).

157. See Amsterdam, *supra* note 150, at 384.

158. See Richard Sobel *et al.*, *The Fourth Amendment Beyond Katz*, *Kyllo and Jones: Reinstating Justifiable Reliance as a More Secure Constitutional Standard for Privacy*, 22 B.U. PUB. INT. L.J. 1, 23–24 (2013) (noting the difficulty for an expectation-based test raised by the fact that “[e]xpectations of privacy may differ from person to person and from day to day”).

159. See Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at “Understandings Recognized and Permitted by Society,”* 42 DUKE L.J. 727, 737–42, 774 (1993) (reporting findings about expectations of privacy indicating that “the Supreme Court’s conclusions about the scope of the Fourth Amendment are often not in tune with commonly held attitudes about police investigative techniques”).

powerfully argued, it would be odd to see the Fourth Amendment as providing such a right against government collection of our information through surveillance, when the modern regulatory state permits (indeed, even requires) collection of much of the same information in so many other ways.¹⁶⁰ Stuntz noted that “much of what the modern state does *outside* of ordinary criminal investigation intrudes on privacy just as much as the kinds of police conduct that Fourth and Fifth Amendment law forbid.”¹⁶¹

While the focus of this Article is not on the purpose of the Fourth Amendment, it is useful to at least propose one alternative way of identifying the subset of privacy violations that also constitute possible Fourth Amendment violations. The best way to identify such governmental intrusion is to begin with the paradigmatic type of invasion that the Fourth Amendment protects us from: the police “fishing expedition.” This is a kind of investigation that sifts through our property with the aim of finding some contraband, evidence of crime, or other findings that would justify subjecting us to state coercion. We find this type of invasion, for example, in the home search where officials rummage through drawers and papers looking for evidence of crime. We find it also in certain airport or road-block search practices, found unconstitutional by the Supreme Court and other appellate courts,¹⁶² where police stop every traveler or car to see if they happen to find evidence of drug possession. As Judge Kozinski stated in a decision holding such a practice unconstitutional when used at an airport security gate, an airport checkpoint is a tempting place for officers to look for evidence of all contraband, even contraband unrelated to air travel.¹⁶³ Such a checkpoint is “a sieve through which pass the contents of billions of satchels, purses, briefcases and pockets [which] will naturally strain out much that is of interest to law enforcement.”¹⁶⁴ But, while tempting, use of such a checkpoint in this way is unconstitutional.¹⁶⁵ It imposes upon individuals the kind of dragnet search that the Fourth Amendment is

160. William J. Stuntz, *Privacy's Problem and the Law of Criminal Procedure*, 93 MICH. L. REV. 1016, 1017 (1995).

161. *Id.*

162. See, e.g., *City of Indianapolis v. Edmond*, 531 U.S. 32, 41, 48 (2000) (stating that the Supreme Court has never found constitutional a roadblock whose primary purpose was finding evidence of criminal activity).

163. See *United States v. \$124,570 U.S. Currency*, 873 F.2d 1240, 1247–48 (9th Cir. 1989) (holding that a generalized search of passengers' baggage violated Fourth Amendment principles).

164. *Id.* at 1246.

165. See *id.* at 1247–48 (finding that the search was not constitutional under the concepts of an administrative search, a *Terry* stop, consent, exigent circumstances, inventory searches, or border searches).

designed to bar, allowing law enforcement to treat individuals they have no reason to suspect of a crime as potential criminals who, as such, must reveal all of their possessions and papers, as well as their persons, for thorough examination. Airport checkpoints can and are, of course, permissibly used to conduct certain kinds of suspicionless searches—namely, searches of every air traveler for weapons or items that might be used for terrorism.¹⁶⁶ However, such searches are subject to tight constitutional limits.¹⁶⁷

The constitutionality of types of observations by officials can be defined by this kind of paradigmatic analysis. After all, it is not the case that every state intrusion into an individual's privacy, even privacy that we reasonably rely upon, necessarily subjects us to the functional equivalent of the general search or dragnet investigation that was the focus of the Fourth Amendment's protections. Rather, what constitutes a general search is not only that it intrudes upon an individual's privacy, but that it does so in a way that alters an individual's relationship with the state. It converts that individual into a suspected criminal.

This is a concern that is, to some extent, at the core of the key alternatives to a privacy-based account of Fourth Amendment purpose. The Fourth Amendment's purpose is not simply to preserve a certain amount of privacy; it is rather to assure that individual citizens are ordinarily able to keep a certain amount of distance between themselves and the coercive machinery of state power—and live with a certain level of freedom from that power—and freedom from fear of being subjected to it on an official's whim. Professor William Stuntz, for example, argued that the central evil that Fourth Amendment law was designed to combat was not police observation, but police coercion.¹⁶⁸ “[P]rivacy protection,” Stuntz wrote, “has little to do with the worst aspects of police misconduct,” which are about violence towards, or intimidation of, suspects.¹⁶⁹ Using a vehicle search as an illustration, Stuntz argued that when police stop a driver and ask for consent to search the car for drugs, the most worrisome consequence of such a stop for an innocent person subject to the

166. See *United States v. Albarado*, 495 F.2d 799, 803 (2d Cir. 1974) (describing the purpose behind airport searches).

167. See *\$124,570 U.S. Currency*, 873 F.2d at 1247–48 (explaining that airport security searches cannot be used to search for contraband generally or things that “merely look suspicious”).

168. See Stuntz, *supra* note 160, at 1020 (arguing that criminal procedure law's focus on information gathering over police coercion comes at the expense of protecting values).

169. *Id.* at 1078.

search is not that the police will see or examine whatever happens to be in the car; it is “the indignity of being publicly singled out as a criminal suspect and the fear that flows from being targeted by uniformed, armed police officers.”¹⁷⁰ In a similar vein, Professor Jed Rubenfeld has reasoned, based in large part on the Fourth Amendment’s text, that the Amendment’s central purpose was not to assure privacy but security—to protect people from “stifling apprehension and oppression that people would justifiably experience if forced to live their personal lives in fear of appearing ‘suspicious’ in the eyes of the state.”¹⁷¹ Another scholar, Scott Sundby, likewise offered an alternative to the conventional privacy-based account. He stated that the purpose of the Fourth Amendment “is founded upon the idea that integral to the Constitution and our societal view of government is a reciprocal trust between the government and its citizens.”¹⁷² Police, he argued, should not be permitted in our constitutional system to act in ways that treat each citizen as a potential criminal.¹⁷³ For example, police should not be permitted to search for contraband in the trash cans of individuals they have no reason to suspect of criminal wrongdoing.¹⁷⁴

While the exact implications of these non-privacy-based approaches to the Fourth Amendment depend on how they are elaborated, it seems likely that each would justify putting some limits on when and how closely police can track or scrutinize individuals’ activities in a public space. A society where the state tracks a person’s every move, even when it has no good reason to believe he is a criminal, is arguably not showing the kind of trust in its citizenry that Sundby insisted the Fourth Amendment demands.¹⁷⁵ Nor is it likely to leave people feeling secure that, if they obey the law, the government will leave them free from its coercive grasp. A person who feels that the government is always watching for any hint of a legal misstep is likely to feel that a police interrogation and arrest is always a possibility. So Stuntz might find that unconstrained drone tracking carries some of the same harms as arbitrary car searches. And Rubenfeld might find that such ever present drone monitoring generates in its target an

170. *Id.* at 1064.

171. Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 127 (2008).

172. Scott E. Sundby, “Everyman”’s Fourth Amendment: *Privacy or Mutual Trust Between Government and Citizen?*, 94 COLUM. L. REV. 1751, 1777 (1994).

173. See generally *id.* at 1811–12 (summarizing the argument for an approach to Fourth Amendment analysis based on the concept of government-citizen trust).

174. See *id.* at 1788–93 (discussing the lengths the Supreme Court went to in order to justify finding that searches of garbage were outside the Fourth Amendment).

175. See *id.* at 1811–12 (explaining that the trust-based approach better aligns with democratic principles).

intense “fear of appearing ‘suspicious’ in the eyes of the state”—the precise fear the Fourth Amendment’s protections are designed to spare us.¹⁷⁶

Although these accounts often offer an emphasis on trust, security, or freedom from police abuse as an alternative to a privacy-based account of Fourth Amendment purposes, they are perhaps better understood as refinements of such a privacy-based account. State surveillance that threatens Fourth Amendment values, does so in large part because it wrestles privacy away from citizens, leaving the private details of their lives exposed to review and examination by an outside observer. Such a privacy violation is a necessary condition for a state measure to implicate Fourth Amendment interests, at least when the state avoids the kind of trespassory or other interference with property that itself counts as a Fourth Amendment search, but it is not a sufficient condition. Rather, a privacy intrusion generally violates the Fourth Amendment only when it treats an innocent individual as a suspected criminal and thereby makes her more vulnerable to the state’s power of coercion and punishment.

A police investigation that generates and stores records of our public movements and activities creates the effect of treating society as suspected criminals. It not only reduces the privacy of those it records. It also, as Justice Sotomayor explained, allows the government “more or less at will” to review innumerable details of an individual’s life for evidence of possible wrongdoing.¹⁷⁷ As a result, people may be subjected to “arbitrary exercises of police power.”¹⁷⁸

B. Recording as a Dividing Line Between Searches and Non-Searches

Recording should thus be central to Fourth Amendment law because, in the context of public surveillance, it allows authorities to sift through sensitive information about our movements and activities. A recording transforms an ephemeral event into a permanent record. It thus frees authorities from the burden (and cost) of having to observe the public’s movements and activities as they occur. It also removes the challenge of having to remember those movements well enough to compare or combine them with other observations in order to build a larger picture. For example,

176. Rubinfeld, *supra* note 171, at 127.

177. See *United States v. Jones*, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) (discussing the importance of considering a GPS device’s ability to allow recording and aggregation of the details of a person’s movements in determining if there is a reasonable expectation of privacy).

178. *Id.*

the kind of “precise, comprehensive record of a person’s public movements” cannot be easily created unless a GPS unit not only transmits information to police about a person’s whereabouts, but also captures that information in electronic memory.¹⁷⁹ In fact, Sotomayor explained in her concurrence that the fact that the GPS device allows recording and aggregation is precisely what allows the government to discover the private details of public activities.¹⁸⁰

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. As the D.C. Circuit emphasized, with a record of a person’s movements over a several day long period, police can learn things about a person’s life that would be unknown to all other passersby who happen to see that person on roads or streets:

Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one’s not visiting any of these places over the course of a month. The sequence of a person’s movements can reveal still more; a single trip to a gynecologist’s office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story. A person who knows all of another’s travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts.¹⁸¹

The D.C. Circuit did not emphasize the difference between recording and merely observing activities in its opinion. But the difference is important for its argument: it is far more laborious for police to aggregate these details of a person’s activities unless it records each movement or action for later comparison with others. If, in the above example, a particular official does not have a record of the first visit to a gynecologist’s office, it is far less likely he will be able to combine it with the subsequent visit to the baby supply store to infer that the woman is expecting a child. And it is unlikely that he will have access to the earlier detail, unless he is doing all of the tracking himself or working with a team of officers that are constantly sharing information that they have recorded. It is conceivable that even without any recording device, officials could draw an inference

179. *Id.* at 955.

180. *See id.* at 956 (arguing that this factor is important in determining society’s expectation of privacy).

181. *United States v. Maynard*, 615 F.3d 544, 562 (D.C. Cir. 2010) (footnote omitted), *aff’d in part sub nom. Jones*, 132 S. Ct. 945.

from the woman's two visits. However, this becomes more implausible when an investigation aggregates not only two, but tens or hundreds of events.

The latter type of investigation, as Justice Alito stated in his *Jones* concurrence, could hardly have happened in a world before GPS surveillance without "a large team of agents, multiple vehicles, and perhaps aerial assistance."¹⁸² Even in a pre-GPS form of extended location tracking, officials would need to create records of their target's movements in order to share their observations with others on the team.¹⁸³ At least one recent state court decision has treated the fact that one can imagine a more primitive analogue of automated recording as evidence that it cannot be a search. In *Foltz v. Commonwealth*,¹⁸⁴ the Court of Appeals of Virginia held that because "a police officer could have followed and personally recorded the movements of the van" without conducting a search, the use of a GPS recording device to track the van was not a search.¹⁸⁵ But this is not the inevitable conclusion one might draw from such an analogy. It would be extraordinarily difficult for a single officer to follow a van as continuously as a GPS device: it would be an unusual officer, able to forego a significant amount of sleep, who could follow a van driver's every (unpredictable) movement over the course of an entire week. A team of policemen, as Justice Alito recognized, would likely be required, and the fact that one can imagine a much more expensive and complicated low-technology analogue for GPS recording does not mean that GPS recording is not a search.¹⁸⁶

Recording is even more of a game-changing technology for video surveillance than it is in location tracking. When police not only use video cameras on street lamps or drones for real time monitoring, but also to create video surveillance footage that may be subject to later review, they allow for a kind of investigation that is far more intrusive—and far more like a dragnet search—than real-time monitoring. Not only can police aggregate and compare different events or actions, as they can in the context of location tracking, but they can also pause on a particular frame, examine it closely, and

182. *Jones*, 132 S. Ct. at 963 (Alito, J., concurring in the judgment).

183. See *infra* Part II.C (describing the type of traditional police work necessary to record as much information as a GPS device).

184. 698 S.E.2d 281 (Va. Ct. App. 2010), *aff'd*, 732 S.E.2d 4 (Va. 2012).

185. See *id.* at 291–93 (reasoning that the use of GPS technology did not provide a substitute for police behavior that would have otherwise violated a right to privacy because the police could have followed and personally recorded the movements of the van).

186. *Jones*, 132 S. Ct. at 963–64 (2012) (Alito, J., concurring in the judgment).

notice small details of a person's appearance or action that they would be very unlikely to notice if they had only one chance to perceive and remember an event as it occurred.

At the extreme, a recording could create the kind of science fiction world Lewis Padgett depicted in the story, "Private Eye."¹⁸⁷ This is a world in which *every* action we take is recorded and stored in police-owned video footage and in which officials can therefore watch the day-to-day existence of any individual the way most people watch a DVD or downloaded movie—by watching it unfold on a screen and pausing to rewind and review sequences that they did not fully perceive or understand the first time through.¹⁸⁸ If officials subjected an individual who they have no reason to suspect of a crime to this kind of video review just to see if the video record happened to reveal anything suspicious, there is little question that they would be poring over personal details of that person's life in much the same way they do in a more traditional "dragnet" search.

Moreover, what is significant about video recording for Fourth Amendment purposes is not only the way it allows authorities to aggregate and compare many small details of our day-to-day lives, but also the power it gives them to pause on or review the same detail over and over again. We normally miss a good deal of what is happening in a scene in front of our eyes. Typically, people do not consciously perceive elements of a scene that they have no need to notice.¹⁸⁹ Video recording, by contrast, captures the information our perception misses. It replaces our flawed natural memory with an artificial replacement that lacks its imperfections and allows police to overcome its limits.¹⁹⁰ In large part, for this reason, Justice Harlan wrote that even a form of surveillance that is not normally a search,

187. See Blitz, *supra* note 45, at 1350–59 (citing Lewis Padgett, *Private Eye*, in *THE MIRROR OF INFINITY: A CRITICS' ANTHOLOGY OF SCIENCE FICTION* 99 (Robert Silverberg ed., 1970)) (proffering that science fiction has given us a view of the potential future of government surveillance and the need to reconsider the approach to the Fourth Amendment).

188. See Padgett, *supra* note 187, at 100 (describing a fictional "omniscience," which stored a fifty-year history of light and sound images and was "a device for looking into the past").

189. See CHRISTOPHER CHABRIS & DANIEL SIMONS, *THE INVISIBLE GORILLA: HOW OUR INTUITIONS DECEIVE US* 5–7 (2009) (recounting an experiment in which individuals tasked with counting ball passes in a game depicted in a video failed to notice an appearance by an actor in a gorilla suit in the middle of the game); Daniel L. Schacter, *The Seven Sins of Memory: Insights from Psychology and Cognitive Neuroscience*, 54 AM. PSYCHOLOGIST 182, 186 (1999) (explaining experiments in which people fail to perceive significant elements in their environment such as the substitution of a different person for a stranger asking them directions).

190. See Blitz, *supra* note 45, at 1356 (describing how video recordings can be as intrusive as stop-and-frisks).

such as government use of an informant to gather information about a suspected drug dealer or other criminal, should become a search when the informant does not simply listen and remember what he is told, but also electronically transmits and records it.¹⁹¹ There is a constitutionally significant difference, he stated, between “third-party monitoring and recording which insures full and accurate disclosure of all that is said, free of the possibility of error and oversight that inheres in human reporting.”¹⁹² In a world in which individuals gossip about or share what they have observed, our privacy is threatened, but in a way that is often tolerable:

Much off-hand exchange is easily forgotten and one may count on the obscurity of his remarks, protected by the very fact of a limited audience, and the likelihood that the listener will either overlook or forget what is said, as well as the listener’s inability to reformulate a conversation without having to contend with a documented record.¹⁹³

In a world of unrestrained recording, by contrast, there is no comfort in knowing that small and obscure aspects of our conversation will escape notice because recordings can be played over and over again to multiple listeners. We do not have the power to “reformulate a conversation” by offering our own account. The audio recording will provide an authoritative, and virtually indisputable, account. It is thus inevitable, said Justice Harlan, that in a world of unrestrained recording “words would be measured a good deal more carefully and communication inhibited.”¹⁹⁴

In discussing audio recording, Justice Harlan focused primarily on its threat to privacy and its possible chilling effect on communication.¹⁹⁵ For Fourth Amendment purposes, however, what is most worrisome about unconstrained video surveillance (or location tracking for that matter) is not simply that it substantially diminishes our privacy and leads us to refrain from taking spontaneous actions we worry may become part of a permanent record. Instead, it is how this specific kind of diminution of privacy affects each individual’s relationship with state power. While recording by anybody else (including other private individuals)

191. See *United States v. White*, 401 U.S. 745, 787–90 (1971) (Harlan, J., dissenting) (noting that transmitting or transcribing conversations is potentially more damaging to free society than the risk of an informant later reporting on a conversation).

192. *Id.* at 787.

193. *Id.* at 787–88.

194. *Id.* at 787.

195. *Id.* at 787–89.

reduces our privacy to some degree, systematic recording by the government diminishes it even more. It allows the government to systematically analyze aspects of our lives, which, in a liberal, individual rights-based society, are not the government's business. Furthermore, it permits the government to do so with the aim of finding, by chance, some basis for subjecting a person to the far greater degree of police power that has traditionally been reserved for those individuals who officials have reason to think are engaged in criminal activity.

Given these observations about the effects of recording, one might wonder why the test proposed in this Article does not make all government recording a search and instead requires that, to constitute a search, an officer's recording must be "remote," meaning outside the realm that the recording officer can perceive with his eyes, ears, and other senses. After all, Justice Harlan's grave worries about recording seem to apply not just to a drone's recording of events occurring far from the drone's operator, but also to recordings that a police officer makes of what is happening in front of him.¹⁹⁶ Even in a public space, the presence of a government-recording device may chill a citizen's speech or other expressive activity—even if a single police officer operates the device and it is not a part of a massive, surreptitious, surveillance system.

However, for Fourth Amendment purposes, there is an important difference between a police officer recording his own interactions, and that which the government gathers from pedestrians and drivers throughout public space. As suggested above, the point of the Fourth Amendment is not simply to protect privacy, but to prevent the state from engaging in the kind of privacy violation that occurs in a dragnet investigation or other "general search" where the state reaches out and subjects individual actions to extensive or penetrating analysis.¹⁹⁷ By contrast, where recording is not remote—where a camera mounted on a police car simply captures footage of a police officer's interactions at a traffic stop, or a police officer uses an iPhone (or a camera in his uniform) to capture events that occur on a street around him—then the recording is far less amenable to being used to create a searchable archive of an individual's detailed movements and activities. By contrast, "uniform cams," tiny cameras

196. See generally *id.* at 787 (failing to differentiate between transmitting and transcribing of conversations).

197. See *supra* notes 156–72 and accompanying text (explaining that the Fourth Amendment right to privacy is much narrower than the common understanding of the right to privacy and that the Fourth Amendment only seeks to protect unreasonable invasions of privacy, such as police fishing expeditions with no limits).

built into an officer's uniform to record each encounter a police officer has with a citizen, are designed and used to archive the police officer's own encounters with citizens.¹⁹⁸ They are not designed to gather data about innumerable citizen activities happening far from the officer that are unrelated to what the officer is doing.¹⁹⁹ They are intended, as one former police chief puts it, to "collect[] and preserv[e] the best evidence about every encounter between the police officer and the community."²⁰⁰

The larger concern about uniform or dashboard cams is not the privacy threat they raise in each encounter they record, but rather what police might do by technologically enhancing or aggregating such image-capture. If police combine—into a central, searchable data collection—the images that each of them captures on a uniform or dashboard-mounted camera, such action could begin to mimic the effects of a larger recording system. However, a definition of "search" broad enough include any action that could threaten privacy, in combination with other surveillance measures, would cover far too much ground: Virtually any kind of police observation could, in combination with other measures, threaten our privacy and perhaps even allow arbitrary fishing expeditions. A technological form-based or design-based test of the kind proposed in this Article would be of little import if it were this broad.

To be sure, one can imagine scenarios in which police uniform cams or dashboard cams are designed *not* to serve their current purpose of preserving records about each police officer's encounter with the community, but rather to sweep in, and preserve for later review, evidence about citizens' actions and movement. Imagine for example, that instead of mounting a camera that records merely what is in front of the car, police mount a camera like the rotating cameras mounted on top of Google's Street View vehicles,²⁰¹ that constantly captures footage from the 360-degree field surrounding the police car each minute and magnifies each part of this visual field to reveal

198. See Janice Morse, *Tiny Uniform Cams Next Big Thing in Policing*, USA TODAY (May 7, 2013, 6:36 AM), <http://www.usatoday.com/story/news/nation/2013/05/07/tiny-police-cameras/2140483> (noting that the uniform cameras cannot lie and are intended to provide an accurate account of what occurs in the course of police work).

199. See *id.* (discussing how cameras worn on uniforms are the next step beyond dashboard cameras).

200. *Id.*

201. See *Behind the Scenes: Street View*, GOOGLE, <http://www.google.com/maps/about/behind-the-scenes/streetview> (last visited Oct. 12, 2013) (describing how the Google Street View car is capable of taking 360-degree panoramic images to create three-dimensional models of the photographed environment).

details of every person and car passing by. Although such a police car camera technically only captures data from the realm that the officer can potentially see and hear, it might still collect a worrisome amount of data about individual citizens. In fact, such a video surveillance system threatens Fourth Amendment values in the same way as a city-wide system of video recording carried out from stationary cameras or aerial drones: The cameras simply happen to be mounted on police cars rather than on lamp-posts or drones. In such a circumstance, courts should find that police do engage in a search when they use the combined, programmatic use of police car cameras to create, and later review, ongoing records of citizens' movements.

C. Extensions: When Magnification—and Recording—Should Count as Searches and When They Should Not

This Article so far has argued that police conduct a Fourth Amendment search when they remotely record a person's actions or movements, whether they do so with a drone-based camera, a network of street cameras, or a GPS-tracking device. As noted earlier, such *recording enables government officials to search public lives frame-by-frame, much in the way it might search documents file-by-file*. But while remote recording is the clearest type of search in a public space, it is not necessarily the only type. Even in the absence of any recording, police might take advantage of other surveillance technologies to circumvent the traditional Fourth Amendment protection for our "persons, houses, papers, and effects." Using a high-powered telescope, for example, officials gather information from the inside of a person's home that they might otherwise obtain only by entering the house or the curtilage.

There is certainly precedent for the Supreme Court to classify a form of surveillance as a "search" when it is the functional equivalent of surveillance that would be a search. In *Kyllo*, the Court found that police engaged in a search of a home when they pointed a thermal imager at the home from the street outside to measure the heat emissions in order to determine if there likely was a marijuana-growing lamp within.²⁰² This was not, of course, a traditional home search: the officers never entered the house.²⁰³ They simply measured the heat leaking through its walls from a public street where they had every right to be without a warrant.²⁰⁴ The Supreme

202. *Kyllo v. United States*, 533 U.S. 27, 29, 34 (2001).

203. *See id.* at 30 (noting the search was performed from the passenger seat of the agent's car).

204. *See id.*

Court nonetheless held that these heat measurements from the outside were a search, largely because their intrusion into the home was functionally equivalent to a home entry.²⁰⁵

In fact, this concept of functional equivalence was built into the test that the Supreme Court proposed for how to apply the Fourth Amendment to the use of “sense enhancing” technologies to observe the home. The Court held that the use of such technology counts as a search when it is employed to obtain information that otherwise could have been obtained only through “physical ‘intrusion into a constitutionally protected area.’”²⁰⁶ The Court added the caveat that this applies only to technology that “is not in general public use.”²⁰⁷ So while police are subject to Fourth Amendment constraints when collecting heat measurements from the home with a thermal imager, they might be free of such limits if they instead look at the home’s walls with the same kind of binoculars available to bird watchers, sports fans, or amateur astronomers.²⁰⁸ Perhaps this is because unlike thermal imagers, which people do not expect to have pointed at their houses in the course of their normal day-to-day existence, binocular-viewers are a common part of life in modern society, and individuals who wish to safeguard their privacy cannot expect that their activities will always escape magnification by others in their neighborhood. Still, the Supreme Court made clear that it will not allow police to circumvent the Fourth Amendment command that searches of a home be reasonable.²⁰⁹ Invading the home technologically from outside its walls is as much a Fourth Amendment search as invading it physically.

Public surveillance might sometimes cross a Fourth Amendment line and trigger reasonableness requirements, not only when it involves magnification of in-home activities, but also when it is the functional equivalent of other categories of searches. For example, if

205. See *id.* at 33–34 (basing their finding on the fact that the sensors provided information that otherwise only would have been obtainable by physical intrusion).

206. *Id.* at 34 (quoting *Silverman v. United States*, 365 U.S. 505, 512 (1961)) (internal quotation marks omitted); see also *Florida v. Jardines*, 133 S. Ct. 1409, 1419 (2013) (Kagan, J., concurring) (finding that use of a drug detecting dog to alert to drugs inside the house uses a sense-enhancing “device” to invade the house in a way equivalent to a home entry).

207. *Kyllo*, 533 U.S. at 34.

208. It is not clear how the Supreme Court would rule on this. In *Kyllo*, the Court noted that use of technological enhancement had not been completely resolved. *Id.* at 33. In upholding the use of magnification in *Dow Chemical Co.*, the Court noted that an important factor was that the area photographed was not near a home. *Dow Chem. Co. v. United States*, 476 U.S. 227, 237 n.3 (1986).

209. See *Kyllo*, 533 U.S. at 34 (analyzing the search of a home using thermal images for reasonableness)

future police officers use a zoom camera to hone in on a person's pockets or wallet, or the book or letter he is holding in his hand, such public surveillance can reveal to police what they could otherwise learn only by physically rummaging through his pockets or wallet, or asking him to hand over the book or letter for official review. If so, then such magnification would arguably allow police with sense-enhancing technology to do what they could otherwise do only with a search of a person, his papers, or his effects. Under those circumstances, perhaps, the Supreme Court should react as it did in *Kyllo*. Just as the Court did not permit government officials there to collect, from afar, information about the home's interior life that it could otherwise have taken only by physical entry, it might similarly bar officials from collecting difficult-to-observe details about a person or what he is carrying that they could otherwise obtain only by stopping a person and searching his belongings.²¹⁰

In fact, such a stance on magnification could help explain the Supreme Court's otherwise puzzling statements in the aerial surveillance cases. As noted earlier, the Court in those cases suggested that observation of a home's curtilage from planes and helicopters normally raised no Fourth Amendment concerns but might well do so if they captured "intimate activities."²¹¹ This activity-based criterion for aerial searches seems at odds with the way the Court normally analyzes searches in or around a home. After all, when courts ask if police need a warrant to enter a home, they do not ask whether the home search is aimed at uncovering intimate details or more impersonal information.²¹² Rather, they assume, as Justice Scalia explained in *Kyllo*, that "[i]n the home, . . . all details are intimate details"²¹³ and, on that basis, require a warrant for any entry

210. One might object that such functional equivalence is a false one. High-powered magnification, for example, might be the high-tech equivalent not of what a police officer does when he seizes and reviews personal effects or documents (a search), but rather of what he does when he takes a furtive glance at someone's reading materials or possessions from a nearby seat in a restaurant or park. High-powered amplification likewise might be more akin to listening to the personal argument between a nearby couple than it is to intercepting a phone call between them. But where telescopic viewing or amplification gives an official a covert way to observe what they would otherwise have to do by being present, this technological shift in the challenge they face should make a constitutional difference.

211. See *supra* text accompanying notes 124–134; see also CHRISTOPHER SLOBOGIN, *PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT* 59, 62 (2007) (mentioning factors that courts consider when determining whether surveillance of a home's curtilage is too invasive and observing that surveillance of a home's interior would entail different, heightened protections).

212. See, e.g., *Payton v. New York*, 445 U.S. 573, 590 (1980) ("[T]he Fourth Amendment has drawn a firm line at the entrance to the house. Absent exigent circumstances, that threshold may not reasonably be crossed without a warrant.").

213. *Kyllo*, 533 U.S. at 37.

into the home. If, as the Supreme Court has sometimes phrased it, a backyard or other curtilage surrounding the home receives Fourth Amendment protection because it is an “extension of [the] home,”²¹⁴ then why treat its protection as variable? Why understand the curtilage’s Fourth Amendment shield to protect some of the activity that police can observe from a public vantage point but not other kinds of activities that occur in the same location and are just as open to observation? One possible answer is that, if the Court protects intimate details in the curtilage from scrutiny by high-powered drone cameras, it is because they are the kinds of details that police could not traditionally and typically learn without searching a person, her house, her documents, or her effects. Such a rule might also make sense because just as people cannot prevent certain evidence of in-home activities from leaking out—for example, in the form of heat emissions—they also cannot completely and continuously conceal their private documents and personal items from exposure to the outside world. Individuals in the modern world will occasionally have to read an e-mail or mark-up a memo as they ride on a subway or sit in an airport. They will occasionally read a book as they rest in a park or a plaza or check the readings on a personal fitness monitor as they walk through a public space.

The fact that individuals have little choice but to bring these items into public space, where powerful cameras may magnify them and give officials a closer look, does not mean that they are fair game for untrammelled official scrutiny. The Supreme Court noted in *New Jersey v. T.L.O.*²¹⁵ that even when students enter the closely supervised and monitored environment of a school, they often have no choice but to bring with them numerous personal items, including “keys, money, and the necessities of personal hygiene and grooming,” as well as “photographs, letters, and diaries.”²¹⁶ The Court emphasized that these items remain protected from arbitrary searches, even in the tightly controlled confines of a school.²¹⁷ It is hard to see why

214. See *Florida v. Jardines*, 133 S. Ct. 1409, 1414–15 (2013) (“[T]he curtilage of the house . . . enjoys protection as part of the home itself.”); *United States v. Dunn*, 480 U.S. 294, 300 (1987) (outlining the historical origins of the idea of curtilage in common law); see also *id.* at 307 (Brennan, J., dissenting) (agreeing that “curtilage is the area which extends the intimate activity associated with . . . a man’s home and the privacies of life” (quoting *Oliver v. United States*, 466 U.S. 170, 180 (1984)) (internal quotation marks omitted).

215. 469 U.S. 325 (1985).

216. *Id.* at 339.

217. See *id.* at 339–43 (striking a balance in schools between permitting entirely arbitrary searches and requiring warrants for every search).

students (or other individuals) would lose such protection in a public space.

The same is true of cell phone conversations. Conversations that once took place entirely over phone lines between home phones, office phones, and pay phones now increasingly take place over cell phones, often as one or both speakers are walking down the street, waiting at an airport, or sitting in a coffee shop. It seems odd to think that a modern-day *Katz* could be constitutionally subjected to electronic eavesdropping by government officials armed with parabolic microphones or other sound amplification devices because the private conversation he had to conduct from a phone booth on the street in 1967 would today take place over a cell phone call from the same street. Thus, Professor Wayne LaFave's proposal that the Fourth Amendment be understood to protect against use of hidden microphones or recording devices, even in public space, seems justified.²¹⁸

To be sure, *Kyllo*'s doctrine of functional equivalence should be applied with caution: Every police method that uncovers details about a suspect is, at a high level of generality, functionally similar to other methods of uncovering the same details. Police unable to obtain evidence of a drug conspiracy from a suspect's home will have to try to find evidence of the conspiracy elsewhere, such as in public space or in third-party records. The match between evidence sought outside the home, and that which is inside the home, does not—and should not—automatically transform the public, or third-party record, surveillance into a search.

One key advantage of the technological form-based or design-based test proposed in this Article is that it provides a clearer line between searches and non-searches in a public space—and this line would be easily blurred if the doctrine of functional equivalence were applied too freely. Consider, for example, the difficulties that might arise if courts not only accepted this Article's proposal to count remote recording as a search, but also classified as a search all techniques they found to have effects equivalent to remote recording. Consider, for example, the type of search that Justice Alito identified

218. See 1 WAYNE R. LAFAVE, *SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT* § 2.2(e), at 442–43 (3d ed. 1996) (suggesting that privacy expectations are more reasonable for private conversations that take place in a public place than for actions that take place in public space); see also Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 36 (2004) (considering a “presence of electronic surveillance” test under which “any conversation a police officer could hear unaided would not be private, but those that required a wiretap or a bug would be constitutionally protected”).

as an earlier-era equivalent of GPS tracking: an operation that follows a suspect's movements with a team of officers, multiple vehicles, and aerial observation.²¹⁹ Even without a recording device, such tracking may threaten to impose a temporary dragnet on an individual. By following his movements and activities from place to place, police may make an observation that gives them justification to move in for a pat-down or an arrest. Or, consider a simpler version of such tracking: one officer tails a person's vehicle, observes what the suspect does when he exits the vehicle and whether he goes into any particular offices or homes. The officer then reports his observations by cell phone to another officer at the station house, who writes down any observations that either of the officers believes to be of interest. Such observation and dictation might produce, with less advanced technology, records equivalent to those captured with automated video recording or location tracking.²²⁰ Or, in a situation more akin to the GPS tracking in *Jones*, police could use a GPS-tracking device that transmits to the police station, but does not record, the location that a car is in at a particular moment.

In such circumstances, it is plausible that a court intent on safeguarding Fourth Amendment interests would classify the systematic tracking that takes place as a search, even in the absence of an automated recording. Doing so may seem necessary to block police from circumventing the limits that apply to recording. However, it is not clear, why, if police become subject to Fourth Amendment requirements when they follow a person with multiple vehicles for a day, they do not likewise engage in a Fourth Amendment search for twenty minutes. All such tracking potentially raises some of the same dangers raised by ongoing recording of a person's movements. But that does not mean all of it should count as a "search." And the same problems that make the mosaic theory problematic also confront a proposal to count police tracking as a search only when it goes on long enough or involves a certain number of vehicles or officers.

219. See *United States v. Jones*, 132 S. Ct. 945, 963–64 (2012) (Alito, J., concurring in the judgment) (describing what would have been needed to accomplish the search before the advent of GPS-tracking technology).

220. Indeed, when Justice Harlan insisted that there is a constitutionally significant difference between "third-party monitoring and recording," *United States v. White*, 401 U.S. 745, 787 (1971) (Harlan, J., dissenting), the "recording" that so disturbed him was this kind of primitive record creation. Instead of secretly audio recording his conversation with the target of the investigation, the informant wore a bug that transmitted the conversation to an officer outside who surreptitiously listened and then testified after the informant disappeared. *Id.* at 746–47 (plurality opinion).

III. OBJECTIONS, ALTERNATIVES, AND LIMITS: DIFFERENT WAYS OF DEFINING A "SEARCH" (AND A "REASONABLE SEARCH") IN PUBLIC

There are two major objections one might offer against this definition of what kinds of investigatory methods count as a "search" in a public space. First, one might argue that it is too restrictive or that it would leave police unable to effectively investigate and deter crime. Second, one might argue that it is not restrictive enough; it places too much police work outside of the Constitution's search and seizure limits, which presents a serious threat to privacy.

A. *The Objection that the Test Leaves Police Needing Greater Freedom To Investigate*

This objection requires a brief examination of how Fourth Amendment reasonableness standards apply to police investigative methods. Focusing on what kind of police activity the Fourth Amendment covers is only the first step in the two-step inquiry courts must undertake to decide if police activity violates the Constitution. The fact that the Constitution and its requirements cover a particular investigatory method does not mean that the search violates the Constitution. Rather, a search is constitutionally impermissible only when it is "unreasonable."²²¹ So, even if GPS tracking or video surveillance in public counts as a search, courts will allow such surveillance when it is reasonable.²²² Traditional searches, such as home entries, are reasonable only if police first obtain a warrant based on probable cause.²²³ This was also what the Supreme Court assumed police would have to do if they wished to attach a GPS device to a car to track the driver's movements, as they did in *Jones*.²²⁴ However, obtaining a warrant will not always be practical. In fact, it is implausible to require camera operators to obtain a warrant each time they record citizens' activities in public streets. Some existing camera systems collect data continuously and such warrantless operation of video surveillance is often necessary to its effectiveness. Police cannot be expected to seek a warrant for video images the value of which is apparent only after a crime has occurred, as was the

221. *Maryland v. Buie*, 494 U.S. 325, 331 (1990) ("It goes without saying that the Fourth Amendment bars only unreasonable searches and seizures."); *see* U.S. CONST. amend. IV.

222. *See Buie*, 494 U.S. at 331–32.

223. *See Payton v. New York*, 445 U.S. 573, 586 (1980) ("[S]earches and seizures inside a home without a warrant are presumptively unreasonable.").

224. *See Jones*, 132 S. Ct. at 948–49 (finding that a valid warrant is necessary for a Fourth Amendment search to be reasonable).

case in the 2013 Boston Marathon bombing investigation and in the earlier July 2005 investigation of the London subway bombings.²²⁵

One possible response is to argue that this kind of video surveillance should not count as a search at all because, unlike the GPS surveillance in *Jones*, it does not target any particular person. Instead, it routinely collects information from the streets in the event that the camera's images reveal a crime, a threat to public safety or capture evidence later needed for a criminal investigation.²²⁶

The problem with this objection is that it ignores the ways in which general collection of evidence can bring the state one step away from a targeted investigation and undermine Fourth Amendment interests even before it reaches that targeting stage. Consider, for example, a hypothetical police program which uses a thermal imager to collect heat measurements from all houses in a particular region in the event that police, at a later time, decide to search the information for evidence of marijuana-growing heat lamps or other evidence of criminal activity that might be found in the heat measurements. If, as the Supreme Court ruled in *Kyllo*, police engage in a search when they point a thermal imaging device at a single house they suspect of housing marijuana, they must *also* engage in a search when they point that device at many houses and lack any particular suspicion about the residents of those houses. Even if they do not intend to examine the heat measurements they collect until some unspecified later date and are not sure what they will find, they will still have crossed the line that, according to *Kyllo*, makes their investigatory activity a search.²²⁷ Their general search has collected evidence from the interior of a home that they could not otherwise have obtained except by entry into the home. Likewise, if instead of attaching a GPS unit to a particular car as they did in *Jones*, police surreptitiously tacked such units onto hundreds of cars parked in a city sidewalk to see (at some unspecified later time) if any of them moved in patterns characteristic of a drug dealer or purchaser, it is hard to see why the

225. See Keith Proctor, *The Great Surveillance Boom*, CNNMONEY (Apr. 26, 2013, 4:56 PM), <http://management.fortune.cnn.com/2013/04/26/video-surveillance-boston-bombings> (documenting the challenges of using video surveillance to investigate and prevent incidents such as the Boston Marathon and London subway bombings).

226. See, e.g., Allison Linn, *Post 9/11, Surveillance Cameras Everywhere*, NBCNEWS (Aug. 23, 2011, 7:38 AM), http://www.nbcnews.com/id/44163852/ns/business-us_business/t/post-surveillance-cameras-everywhere (asserting that officials typically use security cameras not to catch terrorists, but to gather evidence of wrongdoing and apprehend common criminals); Proctor, *supra* note 225 (observing that cameras do little to prevent crime and instead aid in collecting evidence on criminals once a crime has already occurred).

227. See *Kyllo v. United States*, 533 U.S. 27, 40 (2001).

general version of such an investigation would be any less a search than the targeted variant that actually occurred in *Jones*. Indeed, some courts have argued that it was this type of general surveillance that the Supreme Court in *Knotts* suggested would be especially problematic.²²⁸ In *Knotts*, the Court stated that while it was not a search to track a driver on public roads with use of a single beeper, it might be a search if police used such technology to conduct “dragnet-type” surveillance involving “twenty-four hour surveillance of any citizen of this country.”²²⁹ Consequently, if video or other recording of remote activities is a search when it targets a particular individual, it should be just as much a Fourth Amendment search when police record many individuals’ activities and movement before (even long before) they decide upon whom to focus.

That does not mean, however, that police absolutely need a warrant or individualized suspicion to record activity in public space.²³⁰ As Christopher Slobogin argued, courts analyzing video surveillance could adapt certain aspects of their case law on roadblocks, where courts have relaxed warrant and individualized suspicion requirements; in these circumstances, they nevertheless insisted that officials incorporate privacy protections into their searches.²³¹ Likewise, as argued previously, if obtaining a warrant is impossible for police using ongoing video surveillance, they might instead have to satisfy the kind of “constitutionally adequate substitute for a warrant”²³² that the Supreme Court has sometimes demanded in certain school or workplace search cases, or other situations where officials are using searches to meet a need beyond ordinary law enforcement purposes.²³³ In these cases, instead of

228. See, e.g., *Jones*, 132 S. Ct. at 952 & n.6 (deciding the case on a trespassory standard but noting that under a reasonable expectation of privacy standard, *Knotts* indicates that “dragnet-type law enforcement practices,” like those involved in GPS tracking, might be problematic (quoting *United States v. Knotts*, 460 U.S. 276, 284 (1983))).

229. *Knotts*, 460 U.S. at 283–85.

230. See *Terry v. Ohio*, 392 U.S. 1, 20 (1968) (explaining that warrant and probable cause requirements may not apply to certain types of searches or police activities because such requirements are impractical under the circumstances); see also *New Jersey v. T.L.O.*, 469 U.S. 325, 338–41 (1985) (dispensing with the warrant and probable cause requirements in school settings, but refusing to lower the standard to that applicable in the prison setting).

231. Slobogin, *supra* note 38, at 288–90.

232. *Donovan v. Dewey*, 452 U.S. 594, 603 (1981).

233. See, e.g., *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 650, 664–65 (1995) (finding mandatory drug testing of student athletes constitutional); *Nat’l Treasury Emps. Union v. Von Raab*, 489 U.S. 656, 660–61, 664–68 (1989) (upholding drug testing for hiring and promoting employees for certain U.S. Customs Service positions); *Skinner v. Ry. Labor Execs.’ Ass’n*, 489 U.S. 602, 606, 620–21, 624 (1988) (“The Government’s interest in regulating the conduct of railroad employees to

requiring that police have individualized suspicion, the Supreme Court has required other, system-wide privacy protections. These protections often emphasize (1) standardization, (2) unintrusiveness, and (3) clear necessity given a serious security risk.²³⁴ This ensures that officers have minimal discretion in their searches and that the searches are brief, reveal little information, and can often be avoided easily; given the obvious necessity, determination by a neutral magistrate would be excessive under the circumstance.²³⁵ While this Article does not explore how such “warrant substitutes,” which have typically applied outside of the criminal context, would apply to police use of public surveillance to pursue law enforcement objectives, such an adaptation is possible. Classifying video surveillance as a search does not mean that it will be an option only when police already have the probable cause that they believe the video surveillance itself will give them.

B. The Objection that the Test Leaves Government with Too Much Opportunity for Unjustified Surveillance

1. Expanding the definition of a “search” to cover other privacy intrusions by government

While this Article argues for an extension of the Fourth Amendment to cover public surveillance, there is potentially a significant amount of public surveillance that the proposed test would not cover. Consider, for example, a situation in which a police officer decides to spend an hour following a person whom she notices traveling down the street. Imagine that, while doing so, the officer snaps a picture or takes some video footage with an iPhone or digital camera, but does not use an optical zoom lens to magnify the camera’s image. While such image capture would involve recording, the officer would not be recording *remote* activities; she would not be recording events outside of her presence. Nor would she be engaging in the functional equivalent of remote recording when she engages in close observation only of events within her field of view.

For some scholars, judges, or lawyers, this limit on Fourth Amendment coverage may well be unjustified. Indeed, Christopher

ensure safety, like its . . . operation of a government office, school, or prison, . . . may justify departures from the usual warrant and probable-cause requirements.”); *T.L.O.*, 469 U.S. at 340–41 (explaining that a warrant requirement and a “reasonable grounds” for suspicion standard would both be inappropriate to maintaining order in schools).

²³⁴ Blitz, *supra* note 45, at 1457–58.

²³⁵ *Id.*

Slobogin presented a thoughtful case for defining a Fourth Amendment search more broadly than presented in this Article.²³⁶ More specifically, he offered two types of arguments for a broader definition of “search”: one argument focused on interpreting the Fourth Amendment itself and the other in a suggested surveillance statute which, because it is a statute, may cover more territory than the Fourth Amendment itself.²³⁷

Slobogin’s argument about the Fourth Amendment’s coverage is largely based on the notion that the core purpose of the Amendment is to protect what the Supreme Court has said that it protects since *Katz*—namely, individuals’ actual and reasonable expectations of privacy.²³⁸ Understanding the scope of the Amendment’s protection therefore requires understanding what these expectations are. As Slobogin has argued in an article co-authored by Joel Schumacher, this is a task that demands not merely armchair reflection, but collection of evidence about how Americans actually think about their privacy.²³⁹ Based on this work, he wrote that individuals expect far more privacy than the Supreme Court has recognized in its Fourth Amendment cases, finding, for example, that video surveillance of the kind that appears to be outside the Supreme Court’s definition of a search is more intrusive than investigatory methods that the Court has labeled a search.²⁴⁰ In short, he argued that the Court has refused to categorize as searches “a vast array of investigative techniques” that clearly threaten individuals’ widely shared expectations of privacy, including public surveillance techniques people clearly view as invasive.²⁴¹

236. See 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 1, 13–15 (2012) (suggesting that courts define a Fourth Amendment “search” as a layman would and that a proportionality principle should apply when determining the necessity of a warrant or other protective measures).

237. See generally *id.* at 5–32 (analyzing Fourth Amendment jurisprudence and tests, redefining “search,” laying out a statutory scheme, and commenting on the proposed provisions).

238. *Id.* at 5–6, 9–13 (rejecting property as the best foundation for privacy laws and advocating for a broader definition akin to *Katz*’s reasonable expectation of privacy standard); see also Slobogin, *supra* note 38, at 217 (framing the issue in terms of a right to anonymity).

239. See Slobogin & Schumacher, *supra* note 159, at 732 (explaining the need for empirical study and reflection on this issue); see also Slobogin, *supra* note 38, at 271–72, 275–80 (detailing a further study similar to that conducted by Slobogin and Schumacher).

240. See SLOBOGIN, *supra* note 211, at 33, 110–13 (noting that in many cases, “a wide chasm exists between the Court’s holdings and our subjects’ intrusiveness rankings”); see also Slobogin, *supra* note 38, at 271–72, 275–80 (detailing his more recent empirical study).

241. SLOBOGIN, *supra* note 211, at 31–32.

Slobogin's statutory proposal is even more extensive.²⁴² The definition of "search," in a well-drafted surveillance law, he argued, should cover any "effort by government to find or discern evidence of unlawful conduct."²⁴³ It does not matter whether a police officer looks for such evidence with the aid of technology or "with the naked eye."²⁴⁴ "The officer who watches an individual walking down the street to see what transpires is conducting a search under this definition whether she does so with her unaided vision, binoculars, closed-circuit television, or a drone."²⁴⁵ Slobogin emphasized that focusing on a statutory formulation freed him to "go[] beyond anything the Fourth Amendment requires, in either scope or detail."²⁴⁶ He suggested, however, that this model statute might also help guide and sharpen thinking about Fourth Amendment rules for public surveillance.²⁴⁷

Such a broad definition of a search certainly has some advantages. It is, as Slobogin and other scholars observed,²⁴⁸ closer in many respects to the way a layperson would define the word "search."²⁴⁹ In common usage, a person is typically described as "searching" for something when he is engaged in a focused attempt to find it, regardless of whether he is attempting to do so in a house or an open field or whether he has any sophisticated technology to aid him.²⁵⁰ A person can search for a coin dropped on the sidewalk, for example, simply by scanning his surroundings. Moreover, this broad definition of a search deprives unscrupulous—or heavily pressured—government officials of the temptation to circumvent Fourth Amendment requirements simply by shifting to technologies or strategies that are unfamiliar to the courts. Under Slobogin's all-

242. See Slobogin, *supra* note 236, at 16–34 (expounding on the definitions and substantive rules for various types of searches).

243. *Id.* at 17.

244. *Id.* at 18.

245. *Id.*

246. *Id.* at 5.

247. See *id.* at 4–5 (indicating that one purpose of his article was to resolve debates about which Fourth Amendment theories might serve as alternatives to the "mosaic theory").

248. See Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 768 (1994) (arguing that "scanning [a] crowd," even in public, counts as a "search," but that such a search is clearly constitutional); Stephen E. Henderson, *Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search*, 56 MERCER L. REV. 507, 544 (2005) (arguing that search and seizure "are (and were, at the time of the founding) ordinary, commonplace words" and should "bear that ordinary meaning").

249. *Id.* at 13, 17.

250. See *Search Definition*, MERRIAM-WEBSTER, <http://www.merriam-webster.com/dictionary/search> (last visited Oct. 12, 2013) (defining "search" as "look[ing] into or over carefully or thoroughly in an effort to find or discover something").

methods-covered definition, officials cannot hope to free themselves from legal restraints by substituting far-away drone observation for trespassory GPS tracking or by foregoing advanced surveillance technology and instead using more old fashioned methods of tracking a driver. No matter what methods they use to track or watch a person over time, the Fourth Amendment will cover their investigatory observations.

The problem with such a broad definition of a “search,” however, is that if it were made the basis of a constitutional rule, it would likely impose Fourth Amendment constraints on virtually every observation that police make. Simply by noticing and watching an event that seems, to an officer, to merit closer attention, that officer would place himself on Fourth Amendment territory. This, however, is a counterintuitive way to think about how the Fourth Amendment operates. The Amendment’s language is not designed to constrain everything a police officer sees or focuses her attention on, however temporarily or casually. Instead, it is written to cover a particular subset of police activity—namely “searches” of particular targets: “persons, houses, papers, and effects.”²⁵¹ It makes sense, therefore, to treat as a search circumstances in which police enter, or otherwise physically explore, a person, her house, or her documents and property. It also makes sense to treat as a search circumstances in which police use technology to investigate an object without touching or entering it, for example, by magnifying it or creating a continuous record of its activity from a remote location.

One alternative is to limit the definition of search by focusing on a police officer’s motives rather than his methods. Christopher Slobogin’s definition of search, for instance, arguably includes a motive requirement because it technically applies not to every observation a government official makes, but only to those observations that are part of “[a]n effort . . . to find or discern unlawful conduct.”²⁵² But it is not clear how such a motive requirement would place any significant limitation on Fourth Amendment coverage. The central mission of the police is to watch for and respond to unlawful conduct, and when they attend to a person or event while they are on duty, it is likely that a court will presume they are doing so as part of their job description. In fact, without such a presumption, the line between searches and non-searches will rest on the outcome of a difficult inquiry into hidden

251. U.S. CONST. amend. IV.

252. Slobogin, *supra* note 236, at 17.

subjective motives—of precisely the sort that the Supreme Court has been intent on avoiding in the context of determining whether police have probable cause for a traffic stop and automobile search.²⁵³

A more modest expansion for the test described above would apply Fourth Amendment limitations to all recordings, or record creation in general, rather than covering only remote police recording. Even when an officer simply snaps an iPhone photo of what is directly in front of her, one might argue, she engages in a search. The Fourth Amendment might give her more leeway to conduct such a simple, relatively unintrusive search than it gives a team of officers operating a drone-based camera or collecting and reviewing footage from a city-wide surveillance system. But such leeway would still be limited by search and seizure protection that would, for example, forbid capturing iPhone pictures of people or events that she has no reason to suspect have any connection to criminal activity.

There is, however, a problem with a rule that makes any police observation a search as soon as it is accompanied by even the simplest kind of record creation. Police activity that precisely mirrors that which individuals engage in every day would be converted into a matter of constitutional law. Thanks to the miniaturization of cameras and their incorporation into the cell phones, individuals carry cameras with them almost everywhere, and there are few activities in public spaces that are off-limits to photo and video recording. In fact, police have often found themselves being video recorded by citizens wielding iPhone cameras or other recording devices, and a number of appellate courts have found that individuals have a First Amendment right to record police in this way.²⁵⁴ It is conceivable that the same individual who has a constitutional right to record police officers also has a constitutional right to *avoid* being video recorded by the same police officers they are video recording.

253. See *Whren v. United States*, 517 U.S. 806, 811–13 (1996) (asserting that the Court has never invalidated a Fourth Amendment search based on an officer's subjective motive and that the Fourteenth Amendment provides the appropriate protections for challenging discriminatory police behavior).

254. See, e.g., *ACLU of Ill. v. Alvarez*, 679 F.3d 583, 586–87 (7th Cir. 2012) (holding that an Illinois eavesdropping statute that would ban nonconsensual audio-recording of public officials likely fails intermediate scrutiny and infringes on First Amendment rights); *Glik v. Cunniffe*, 655 F.3d 78, 82 (1st Cir. 2011) (emphasizing that there is a constitutional right to record police in the course of their public duties because public recording of government officials can play an essential role in stimulating “the free discussion of governmental affairs” and protection of freedom (quoting *Mills v. Alabama* 384 U.S. 214, 217 (1966))); *Smith v. City of Cumming*, 212 F.3d 1332, 1333 (11th Cir. 2000) (explaining that “[t]he First Amendment protects the right to gather information about what public officials do on public property, and specifically, a right to record matters of public interest,” including a right “to photograph or videotape police conduct”).

But such a rule has problematic implications. Unlike remote recording with drone cameras or citywide video systems, using an iPhone to snap a photograph of one's surroundings is, in many respects, simply a modern form of note taking. As Professor Seth Kreimer wrote while arguing for extending First Amendment protections to image capture, "[r]ecorded images can serve the same function" as the "sense impressions or . . . sketches in [a] diary."²⁵⁵ It seems unlikely that the Fourth Amendment places police on constitutional territory every time they supplement their own perception or memory in the way that ordinary citizens do every day.

In fact, the desire to avoid such a result was likely what caused the Supreme Court to note in *Kyllo* that use of sense enhancement technology probably would not count as a search when that technology was "in general public use," unless it were aimed at a house or other private environment.²⁵⁶ The "general public use" test has been the target of scholarly criticism,²⁵⁷ and critics are right to argue that the Supreme Court would invite chaos and confusion if what counted as a search changed each year as new technologies and cultural practices transformed the way people interact with public space.²⁵⁸ But whatever its flaws as a black letter law test, the general public use requirement at least captures a powerful intuition about Fourth Amendment law: it should not subject *all* police observation and record-creation to heightened judicial scrutiny. The question rather, is what kind of police monitoring in public must be subject to Fourth Amendment limits and what kind of garden-variety police observation remains free of such limits. It is probably implausible to

255. Seth F. Kreimer, *Pervasive Image Capture and the First Amendment: Memory, Discourse, and the Right To Record*, 159 U. PA. L. REV. 335, 380 (2011).

256. See *Kyllo v. United States*, 533 U.S. 27, 40 (2001).

257. See, e.g., SLOBOGIN, *supra* note 211, at 57–58, 62–65 (positing that public use is a blurry line that could refer either to how easily the general public can acquire the technology or to how frequently the general public uses the technology); Douglas Adkins, *The Supreme Court Announces a Fourth Amendment "General Public Use" Standard for Emerging Technologies but Fails To Define It: Kyllo v. United States*, 27 U. DAYTON L. REV. 245, 262 (2002) (criticizing the *Kyllo* "general public use" doctrine as completely unworkable and asserting that "the Court must have intended something . . . other than actual use by the public").

258. See, e.g., David A. Harris, *Superman's X-Ray Vision and the Fourth Amendment: The New Gun Detection Technology*, 69 TEMP. L. REV. 1, 23 (1996) (noting that "[t]he type of technology the public can possess may change with surprising speed"); Tracey Maclin, Katz, *Kyllo*, and *Technology: Virtual Fourth Amendment Protection in the Twenty-First Century*, 72 MISS. L.J. 51, 105 (2002) ("[W]hether a particular device is in general public use should have no impact on Fourth Amendment analysis."); Christopher Slobogin, *Peeping Techno-Toms and the Fourth Amendment: Seeing Through Kyllo's Rules Governing Technological Surveillance*, 86 MINN. L. REV. 1393, 1412 (2002) (observing that courts will have "to deal with the rapid pace of technological development in deciding whether something is in general public use").

insist that police be free from Fourth Amendment limits any time they use a technology that is generally available to private citizens: That would mean that, even as enhancements to aerial drones and GPS units make these devices a greater threat to privacy, their use by police would paradoxically become subject to less Fourth Amendment oversight—as long as private citizens are able to purchase and use such surveillance technology for their own purposes.

Use of these remote recording technologies should count a Fourth Amendment search, but this is not because these technologies are—for the moment at least—less widely used, or available to private citizens, than SmartPhone cameras. Rather, it is because remote recording technologies allow police to do something they cannot easily do with a SmartPhone, which is to generate a “precise, comprehensive record of a person’s public movements”²⁵⁹—a digital archive they can later use to engage in a frame-by-frame search.

The government might conceivably subject U.S. citizens to such a dragnet investigation even without automated recording technology that can follow an individual far from where an officer is positioned. But doing so is likely to be costly and burdensome for police. As Justice Alito stated in *Jones*, tracking an individual over a period of days without GPS technology is likely to require significantly more man power and police resources and is likely to be a far more complex operation.²⁶⁰ As Justice Breyer explained in *Illinois v. Lidster*,²⁶¹ such an investigation may be in less need of constitutional restraint because its costs make it subject to heavy practical restraints.²⁶²

2. *More general technology-centered approaches*

Other scholars have explored ways of defining searches in public space that are less expansive but still arguably cover more ground than the proposed definition offered in this Article. Another set of recent and promising proposals, for example, come from scholars who argued for a technology-based approach to what counts as a search. In contrast, however, they analyze it at a higher-level of

259. See *United States v. Jones*, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring).

260. *Id.* at 963–64 (Alito, J., concurring in the judgment).

261. 540 U.S. 419 (2004).

262. See *id.* at 426 (explaining that there is little cause for concern that its approval of police information stops would lead to “unreasonable” worry about “proliferation of police checkpoints” because “[p]ractical considerations—namely, limited police resources and community hostility to related traffic tieups—seem likely to inhibit any such proliferation”).

generality than in this Article, which focuses on public recording (remote or otherwise) and certain types of magnification and amplification. Professors David Gray and Danielle Citron, for example, argued for a “technology-centered approach” to determine which investigations count as Fourth Amendment searches.²⁶³ Their test would classify *any* technology as a search if it “has the capacity to facilitate broad programs of indiscriminate surveillance that intrude upon reasonable expectations of quantitative privacy.”²⁶⁴ Among the technologies that enable such “pervasive surveillance” are “aerial drones, GPS-enabled tracking, [and] digital dossiers.”²⁶⁵ These technologies, Gray and Citron claim, raise the same specter of authoritarianism for modern citizens that “broad and indiscriminate use of physically invasive searches and seizures” did for our predecessors.²⁶⁶

Another similar approach that inspired Gray and Citron’s proposal is Susan Freiwald’s proposal. Freiwald stated that courts can mark a line between searches and non-searches with a four-factor test that the Supreme Court and other courts have developed over the last four decades in cases addressing wiretapping or video surveillance in homes, offices, or other private spaces.²⁶⁷ Under this test, a method of public surveillance would count as a search when it is characterized by each (or perhaps, most) of the following elements: it is (1) hidden, in that the target is unaware of it; (2) intrusive, in the sense that it “affords law enforcement agents access to things people consider private”; (3) continuous, in that it represents an ongoing “series of intrusions” rather than a single intrusion by the state; and (4) indiscriminate, in that it “gathers up more information than necessary to establish guilt.”²⁶⁸ GPS surveillance, she argued, will typically count as a search under these criteria because GPS units are typically hidden, record myriad details about a person’s movements and activities, do so over an extended period of time, and gather

263. Gray & Citron, *supra* note 32 (manuscript at 5).

264. *See id.* (manuscript at 5) (elaborating that technology that qualifies as a search under this test would then be subject to Fourth Amendment warrant and reasonableness requirements).

265. *Id.* (manuscript at 27).

266. *Id.*

267. *See* Freiwald, *First Principles*, *supra* note 32, ¶¶ 9–11 (outlining the details of the Four Factor Test, its derivation from case law, and how it promotes the goals of the Fourth Amendment); Freiwald, *Four Factor Test*, *supra* note 32 (summarizing how courts essentially apply a four-factor test when analyzing what Fourth Amendment protections should apply to a given investigatory method).

268. Freiwald, *Four Factor Test*, *supra* note 32; *see also* Freiwald, *First Principles*, *supra* note 32, ¶¶ 61–69 (adding that courts could apply lesser standards to those surveillance methods that do not share all four factors).

much information unrelated to criminal activity.²⁶⁹ Surveillance by an unseen drone would count as a search for the same reason. Video surveillance by street cameras is not hidden to the same extent, as pedestrians can often see the cameras on buildings or corners, but it otherwise shares the features that make GPS tracking and drone surveillance a search.

Interestingly, the earlier cases that Freiwald relies upon, which applied similar principles to cases of wiretapping and video surveillance, did not use these criteria to determine whether a certain investigatory technique was a search or a non-search. Rather, courts employed these factors to justify imposing certain “heightened procedural hurdles,” beyond a showing of probable cause, on certain types of unusually threatening electronic searches.²⁷⁰ Still, although these criteria were used to determine what hurdles the government had to overcome to make a search reasonable, they can be adapted to the task of determining what public monitoring should count as a search at all. Although police surveillance in public has traditionally been entirely outside the Fourth Amendment’s coverage, when it raises the same risks for privacy and autonomy as the most worrisome forms of inside surveillance, such as wiretapping or video recording from cameras hidden in homes or businesses, then it makes sense to bring such public surveillance into Fourth Amendment territory so that courts can guard against its possible abuses. Thus, when public surveillance is hidden, intrusive, continuous, and indiscriminate (under Freiwald’s test) or capable of broad and indiscriminate surveillance (under Gray and Citron’s), it is—just as wiretapping and bugging—subject to constitutional limits.

Such an approach has two advantages that might, to some, make it seem preferable to a test that focuses on recording capacity, magnification, or some other specific technological feature. First, it has the virtue of offering a single standard that courts can apply not only to surveillance in public spaces, but to all kinds of wide-scale government surveillance, from wiretapping, to thermal imaging and GPS tracking. Second, like Slobogin’s all-methods-covered approach above, Gray, Citron, and Freiwald’s approaches are broad enough

269. Freiwald, *Four Factor Test*, *supra* note 32.

270. Freiwald, *First Principles*, *supra* note 32, ¶ 10; *see, e.g.*, *Berger v. New York*, 388 U.S. 41, 60 (1967) (developing constitutional rules for electronic eavesdropping in part with a focus on that technology’s “inherent dangers”). As Judge Posner noted in applying such criteria to video surveillance, such surveillance was “inherently indiscriminate” and “could be grossly abused—to eliminate personal privacy as understood in modern Western societies.” *United States v. Torres*, 751 F.2d 875, 882 (7th Cir. 1984).

that they easily apply limits to alternative technologies (or low-tech analogues) that the government employs to circumvent Fourth Amendment limitations. For example, if police try to circumvent a Fourth Amendment restriction on remote recording by sending out officers to continuously record activities on dashboard cameras and then storing them for later analysis, Gray and Citron's test would likely still give courts all of the doctrine they need to classify such recording as a search based on its potential for broad and indiscriminate investigation of citizens' public movements or actions.²⁷¹ Freiwald's test would also likely classify such widespread recording as a search, because it is intrusive, continuous, indiscriminate (and, if people do not see the cameras in the police cars, also hidden).²⁷² Courts thus would not have to analogize this multi-officer use of individual recording devices to hidden surveillance from drones or street cameras.²⁷³

271. See Gray & Citron, *supra* note 32 (manuscript at 5, 12–13, 36) (noting that their technology-based approach to the Fourth Amendment should serve as a guide to prevent unfettered government recording of the public and limit “broad programs of indiscriminate surveillance”).

272. See Freiwald, *First Principles*, *supra* note 32, ¶¶ 9–11 (basing her test on video surveillance cases). Police could use video surveillance technology to continuously record the public in much the same way that drones might. See Freiwald, *Four Factor Test*, *supra* note 32 (applying the four-factor test and concluding that law enforcement officials should seek a warrant before engaging in GPS tracking).

273. Such general approaches offer yet another possible benefit: they may be broad enough to cover government collection and analysis of third-party images and videos. Third-party video records could conceivably provide officials with all the data they need to create detailed archives of individuals' activities. Much of the video used in the Boston Marathon investigation, for example, came from the video cameras of private businesses and individuals filming the Boston Marathon (or the aftermath of the bombing) with their own smart phone cameras. Kelly, *supra* note 1.

Third-party records could be of similar benefit in location tracking. As Stephen Henderson has written, location data has immense value to private businesses, since it allows them to discover customer habits and patterns. Stephen E. Henderson, *Learning From All Fifty States: How To Apply the Fourth Amendment and Its State Analogs To Protect Third Party Information from Unreasonable Search*, 55 CATH. U. L. REV. 373, 383–84 (2006). For example, “a business would probably like to know that customers spend an average of fifteen minutes in the store.” *Id.* at 383–84. Furthermore, a third party's natural interest in location-tracking, combined with the location-tracking capacities “inherent in [cell phone] technology,” make it likely that police will find all the information they need to track an individual in records already collected by private parties. *Id.* at 385. It is thus understandable that the concurring justices in *Jones* were worried not only about officials using public cameras or government-installed GPS devices, but also about government collection and analysis of third-party-generated data. Justice Alito, for example, noted that “[m]any motorists purchase cars that are equipped with devices that permit a central station to ascertain the car's location at any time” and that “cell phones and other wireless devices now permit wireless carriers to track and record the location of users.” *United States v. Jones*, 132 S. Ct. 945, 963 (2012) (Alito, J., concurring in the judgment). Justice Sotomayor explained that a coherent approach to privacy in public may require the Supreme Court “to reconsider the premise that an individual

There are, however, two disadvantages to the more abstract approach. One is the opposite of the advantage discussed above. The same generality that allows these approaches to more easily cover a wide range of investigatory techniques also makes it less predictable which techniques will be covered by the Fourth Amendment. Consider, for example, some of the questions courts would face in assessing whether certain video- or image-capture technology is capable of broad and indiscriminate use (under Gray and Citron's test) or "intrusive" (under *Freiwald's*). In defining how broad, indiscriminate or intrusive a technology is, should courts consider any technological or administrative safeguards (e.g., a rigorously enforced restriction on access) that a police department builds into its video surveillance system?²⁷⁴ Should they consider use of a surveillance technology to be a search if that technology is relatively unthreatening in its typical form but can be easily repurposed so as to let police engage in more intrusive searches? Do police engage in a search, for example, if they use recording systems that blur faces, but

has no reasonable expectation of privacy in information voluntarily disclosed to third parties." *Id.* at 957 (Sotomayor, J., concurring).

Conceivably, a government investigative method that draws on other parties' video footage rather than the government's might still count as a method that facilitates "broad programs of indiscriminate surveillance" under Gray and Citron's test. Gray & Citron, *supra* note 32 (manuscript at 5). Indeed, Gray and Citron suggested that their approach would at least cover situations where a private party was acting as a state agent, and "that in most cases where government leveraging of private data reservoirs would raise [Fourth Amendment] concerns, one or more of the[] tests of state agency" would very likely be met. *Id.* (manuscript at 45–46). Of course, such a state agency test would likely solve the same problem under the narrower approach suggested in this Article.

If it did not do so, and Justice Sotomayor thus remained correct that effective Fourth Amendment protection of privacy requires a reformulation of the third-party doctrine, then such a change to the third-party doctrine would not be sufficient, by itself, to subject government recording of public activities (or analysis of others' recordings) to Fourth Amendment rules. The Supreme Court would also need some rationale and guidance providing why and when video footage captured in open spaces could implicate Fourth Amendment privacy interests even when it occurs in public and observable space. After all, if we do not have any account of why it might be constitutionally problematic for the government to routinely videotape public activities by itself, it would not be clear why it is any more problematic for it to obtain the same information from others. We thus need some approach, like the one this Article offers, to explain when and why government recording of citizens' activities would cross a constitutional line; the approach would also have to explain when and why gathering the same information from third parties' recordings might be unconstitutional. Although a more general technology-centered approach can certainly serve this role, so too can a narrower test that subjects only remote recording and certain instances of magnification or amplification to Fourth Amendment scrutiny.

274. See Gray & Citron, *supra* note 32 (manuscript at 5) (describing its test as one that looks to the potential uses and abuses of the technology as a basis for incurring Fourth Amendment scrutiny); *Freiwald, Four Factor Test*, *supra* note 32 (considering potential limits on GPS tracking).

where police can easily remove the blurring? Or when they use a recording system that can work only if a particular police officer is operating it, but which can easily be reprogrammed to record continuously and automatically?

Gray, Citron, and Freiwald's abstract approaches are also problematic in that it is likely to over-expand Fourth Amendment coverage. Freiwald's proposal, for example, is likely to sweep in more police work than the test proposed by this Article because there are kinds of public surveillance that arguably satisfy all four elements of Freiwald's test but involve neither recording nor substantial magnification of otherwise invisible details on a person, paper, or effect. For example, imagine that an officer in an unmarked vehicle becomes suspicious of a car driving in front of him and decides to follow a few cars behind on the road for a period of ten or fifteen minutes. There is a good chance this counts as a "search" under Freiwald's test.²⁷⁵ While the officer's car is visible, he does not intend to alert the driver ahead that the government is watching her.²⁷⁶ So the officer's observations are hidden. The officer's activities are certainly also continuous. The officer is gathering at least some information about actions that are unlikely to reveal criminal activity. Whether this activity is sufficiently intrusive to be a search is unclear, but without additional guidance for answering this question, courts facing it might encounter the same difficulty that the Supreme Court encountered in *Jones*. Like the proposal in this Article, Freiwald's test avoids making intensity or duration the key determinants of whether an investigation is a search.²⁷⁶ Instead, Freiwald directed courts to apply these factors to each "method of surveillance."²⁷⁷ So courts will have to decide how to define—and judge—the method of surveillance being used in a situation in which the only surveillance technology an officer is using to watch someone is the car he is driving. It is possible that if courts conclude that such observation is typically non-intrusive, they will define it as a non-search even if one can imagine more intrusive variants of it. But courts certainly have more leeway under this test than they do under the test proposed in

275. See Freiwald, *Four Factor Test*, *supra* note 32 (viewing GPS tracking as a search and therefore potentially any attempt by police to track drivers as a search for the same reasons).

276. See Freiwald, *First Principles*, *supra* note 32, ¶ 69 (focusing instead on the continuous nature of a search, not on a specific length of time, and incorporating three additional factors into the test).

277. See *id.* ¶¶ 50, 60 (stating that the courts should also make clear decisions on what the Constitution demands before law enforcement begins using new technologies).

this Article to classify as a “search” visual observation by police officers that is unaided by cameras or other technology.

Still, the approaches offered by Gray, Citron, and Freiwald might well end up leading courts to define the Fourth Amendment territory that the proposal here covers. Remote recording is certainly capable of the broad and indiscriminate use that, for Gray and Citron, is the hallmark of a Fourth Amendment search. Remote recording is also, as a general matter, likely to be hidden from the view of the target; the police officer doing the recording is not present (and the device doing the recording is often not visible). It is certainly continuous, and it indiscriminately captures significant amounts of information unrelated to crime. So it also satisfies Freiwald’s test. High-level magnification of reading materials or other items we assume are private is also likely to occur without our knowledge and to be intrusive and indiscriminate.²⁷⁸

Thus, it is plausible to view the proposal set forth in this Article as a specific application of the approaches discussed by Gray, Citron, and Freiwald, which advocate that the Supreme Court count as a search all public surveillance that eliminates the possibility for “private or anonymous action” in public space.²⁷⁹ Recording remote events and close magnification of details are only two examples of surveillance technologies that raise such concerns.

Yet Courts might offer greater clarity—not just to law enforcement agents but to other courts—if they start with such abstract criteria, but rather with a test that marks remote recording and high-level magnification as searches. This more modest approach also adheres more closely to the Supreme Court’s own precedent on surveillance in public spaces.²⁸⁰ As noted above, the Supreme Court has already stated in its tracking cases that location-monitoring technology may count as a search when used in conjunction with dragnet information-gathering devices; this might include any device, like GPS, that records a person’s movements from one place to another. It has noted in its aerial surveillance cases that even when police observe a home’s curtilage or a business’s open premises from a place where the public has a right to be, their surveillance might still be a

278. Whether it is continuous is less clear. See Blitz, *supra* note 45, at 1383–84 (indicating that magnification of images caught on video surveillance implicates privacy concerns, even if the Supreme Court refuses to lend much credence to such concerns); see also Freiwald, *First Principles*, *supra* note 32, ¶¶ 69–70 (examining the continuousness requirement in relation to e-mails).

279. Blitz, *supra* note 45, at 1446.

280. See e.g., *United States v. Knotts*, 460 U.S. 276, 281 (1983) (noting that people can reasonably expect reduced privacy on, for example, public roadways).

search when it reveals intimate details about a person's life.²⁸¹ Building on such precedent in future cases on public surveillance, the Supreme Court may eventually build the framework that marks particular investigatory techniques as searches or non-searches based upon their general level of intrusiveness or their capacity to indiscriminately and continuously capture information. If and when such a framework emerges, this might also allow a link between the Court's emerging Fourth Amendment jurisprudence on surveillance in public spaces and its jurisprudence on surveillance of Internet and phone communications. Nevertheless, even if the Supreme Court takes a more cautious and minimalist approach, there is a technological form- or design-based approach that allows it to proceed in extending Fourth Amendment protection to public surveillance.

CONCLUSION

In recent years, judges seeking to apply Fourth Amendment law to emerging surveillance technologies have faced a dilemma. On the one hand, if they continue to insist on the simple rule that public space is a Fourth Amendment-free zone, they seem to betray Fourth Amendment purposes.²⁸² While the Fourth Amendment does not, as the Supreme Court noted in *Katz*, establish a "general constitutional 'right to privacy,'"²⁸³ it does protect us from government fishing expeditions whereby police invade the private realms of our life in search of details that would justify subjecting us to an arrest or other seizure.²⁸⁴ Police cannot arbitrarily sift through the items in our house or the documents in our briefcase,²⁸⁵ so it is not clear why they should be able to create, and then sift through, video frames of people's day-to-day movements through public space, especially because even acts that occur in a public space may betray aspects of their lives that are 'deeply private and personal. In fact, roadside cameras or drones might capture evidence not only of citizens'

281. See *supra* notes 124–133, 207 and accompanying text.

282. See, e.g., *United States v. Jones*, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) (emphasizing that the Court must retreat from an idea of privacy as complete secrecy); *id.* at 961 (Alito, J., concurring in the judgment) (observing that the majority's trespassory standard could lead to "incongruous results").

283. *Katz v. United States*, 389 U.S. 347, 350 (1967).

284. See *Camara v. Mun. Court*, 387 U.S. 523, 528–29 (1967) (explaining that the historical purpose of the Fourth Amendment was to preserve the privacy of the home and safeguard against arbitrary government invasions).

285. See U.S. CONST. amend. IV (stating that the government cannot arbitrarily search a person's "houses, papers, and effects" without probable cause); see also *Camara*, 387 U.S. at 528 (prohibiting "arbitrary invasions by the government").

movements, but of their private thoughts. They might give hints about personal internal demons individuals are struggling with when they visit a psychotherapist, twelve-step group, or library. This is especially true if the state not only has a record of its citizens' movements, but also video footage that captures facial expressions, demeanor, gait, and perhaps (with powerful magnification) the documents held in their hands.

On the other hand, if courts extend the Fourth Amendment into the realm of the public and visible, it is not at all clear how far this extension should go. It seems wrong to say that every glance by police or every event they observe in the street suddenly activates a constitutional force field protecting the subject of their attention; it also seems wrong to assume that if police look a bit closer—whether by staring for a longer time, donning a better pair of glasses, or using their binoculars or iPhone—Fourth Amendment protections immediately apply. The concurring opinions in *United States v. Jones* rightly did not let this difficulty deter them from concluding that the Fourth Amendment applies to public space, but they also did not find a way to resolve the issue.²⁸⁶ Rather, they assumed that there is a vague, yet-to-be-identified line between public surveillance that is sufficiently brief to avoid judicial scrutiny of any kind and longer surveillance that might count as a “search.”²⁸⁷

This Article has proposed a way out of the dilemma. First, whether public surveillance counts as a Fourth Amendment search depends not on its duration or intensity, but rather on whether it uses technology that attempts to do what the Fourth Amendment was meant to stop: dragnet surveillance that creates records of activities that police can then sift through for evidence that might justify subjecting us to the coercive powers of the state. In short, this means that the Fourth Amendment should first bar the government from recording with technologies that inescapably follow citizens through public space and record them remotely wherever they can be found—no matter how far they may be from the sight or hearing of a police officer. Whether that recording lasts only a few seconds or a month, it is still a search because, by turning it on, police are

286. *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring) (“I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.”); *id.* at 960–61, 964 (Alito, J., concurring in the judgment) (arguing that the determining factors for Fourth Amendment protection should include the duration of the intrusion and reasonable expectations of privacy, not the presence of a physical trespass).

287. *Id.* at 964 (Alito, J., concurring in the judgment).

subjecting citizens to a technology that is *capable* of creating a digital archive of evidence about their lives. To be sure, its brevity may be relevant to the question of whether it is reasonable. Courts may decide that such brief recording is unlikely to threaten people and should thus be permitted even if police have a level of suspicion that is far lower than probable cause. When the video recording targets no one at all and instead simply sweeps in all people and events that occur in a given area, then courts might likewise give police more leeway to record, as long as it is clear that any attempt to use these recordings to trace the path of a particular person triggers the same warrant (or other) requirements that would limit targeted surveillance in the first instance.

2004

Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World That Tracks Image and Identity

Marc J. Blitz, *Oklahoma City University*



SELECTEDWORKS™

Available at: http://works.bepress.com/marc_jonathan_blitz/15/

Texas Law Review

Volume 82, Number 6, May 2004

Articles

Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World that Tracks Image and Identity

Marc Jonathan Blitz*

Introduction.....	1350
I. The <i>Katz</i> Revolution: Strengthening and Expanding the Protection of Private Spaces.....	1366
II. The Technological Challenge to <i>Katz</i> : Watching, Tracking, Identifying, and Detecting Private Details in Public Spaces	1374
A. Video Surveillance.....	1377
B. Enhancements to Video Surveillance: Tracking, Magnification, and Biometrics.....	1383
1. <i>Tracking</i>	1384
2. <i>Magnification</i>	1389
3. <i>Biometrics and Face Recognition</i>	1390
C. Detection.....	1398
III. Beyond the <i>Katz</i> Test: Protecting Privacy in Public Places.....	1406
A. Privacy Interests in Public Space.....	1406
B. Securing an Architecture for Privacy (Not Just an Instance of It)	1413
C. Reconciling Fourth Amendment Freedom with Technological Progress and Effective Policework	1426

* Associate, Wilmer, Cutler & Pickering, J.D. University of Chicago (2001); Ph.D. (Political Science) University of Chicago (2001). This Article is based on research and analysis conducted for the video surveillance study group of the Constitution Project's Liberty & Security Initiative. The Article benefited from invaluable input and guidance from Joseph Onek, Director of the Constitution Project's Liberty & Security Initiative; Jeffrey Rosen, Associate Professor of Law, George Washington University Law School and Reporter for the Constitution Project's Subcommittee on Privacy and Technology; and David Medine, Partner at Wilmer, Cutler & Pickering. It also benefited from analyses by, and/or discussions with, other attorneys at Wilmer, Cutler & Pickering who worked with the video surveillance study group, particularly Meredith Halama, Lee Milstein, David Engstrom, and Owen Kendler.

IV. Applying Privacy Protections to Public Space: Revising <i>Katz</i> and Refining Justice Harlan's Alternative Framework.....	1434
V. "Reasonable" Warrantless Searches: Using Surveillance Technology Against Terrorism.....	1449
A. Judicial Balancing of Privacy and Security (and Reasonableness Requirements Beyond Balancing)	1449
1. <i>Warrant Substitutes and Minimization</i>	1457
2. <i>Selective Warrants</i>	1464
3. <i>Unmonitored Recording and Carefully-Restricted Viewing</i>	1467
Conclusion	1479

Introduction

In Lewis Padgett's¹ short story, *Private Eye*, it is discovered that the whole of the physical environment doubles as a pervasive recording system: On every wall, every tree, every patch of ground people walk upon, their every action and conversation leaves "'fingerprints' of light and sound waves."² Scientists have learned to "descramble" these naturally created records of people's activities and compile them into video archives containing every individual's entire past.³ Government investigations proceed very differently from those in our own world. Police detectives spend most of their time in a screening room, rewinding and fast-forwarding through each suspect's life.⁴ When they want a closer look, they can slow or pause their film to examine "every expression of his face, every muscular flexion, every breath he [draws]."⁵ When curious about the experiences that have shaped him, they can instantly transport themselves back into his childhood.⁶ Even those not currently under such a government microscope know that each moment of their lives is preserved for "[a]n invisible audience from the future."⁷

The inescapable surveillance that Padgett describes in his obscure 1949 story resembles that described in another more famous science fiction tale published the same year: George Orwell's *1984*. Like George Orwell's

1. "Lewis Padgett" was one of many pseudonyms used by the husband and wife science fiction writing team of Henry Kuttner and Catherine L. Moore.

2. Lewis Padgett, *Private Eye*, in *THE MIRROR OF INFINITY: A CRITICS' ANTHOLOGY OF SCIENCE FICTION* 93, 100 (Robert Silverberg ed., 1970).

3. *Id.*

4. *Id.* at 100-06.

5. *Id.* at 117.

6. *Id.* at 101-02, 122-23.

7. *Id.* at 117.

vision of a technologically transformed future,⁸ the world imagined by Padgett is one where individual privacy is brought by science to the brink of extinction. But unlike the inhabitants of Orwell's imagined world, who have resigned themselves to living without their privacy, the inhabitants of the world described by Padgett have made an impressive and arguably effective effort to save it. They have countered the threat posed by exotic "past-tracing" technology with a not-so-exotic legal device: a rule that past-tracing evidence can be accessed only for purposes of investigating a "serious crime" and introduced at trial "only if it [has] a direct connection with the crime."⁹ Although natural barriers no longer stand in the way of paternalistic or distrustful officials, the law continues to do so: Government investigators are allowed to explore people's pasts only when doing so is indispensable to the task of protecting people or of apprehending those who have harmed them.¹⁰

The courts and legal thinkers of Padgett's time did not carefully examine the effectiveness of such protections, and there was little reason to worry about this question in 1949, when nothing remotely like "past-tracing" technology played a significant part in their day-to-day lives. But the challenge outlined in this story is a more pressing concern now. While the physics of Padgett's imagined world have remained firmly in the realm of fiction (there are no hidden video recordings encoded in wood, stone, or soil), its privacy-eroding technology is not all that far from becoming reality. Walls, lampposts, and trees do not function as natural video cameras, but new technologies allow public authorities to line them with artificial ones. A growing number of communities throughout the world are doing so on a massive scale. The United Kingdom has led the way. Cameras now encircle the center of London in a "ring of steel," photographing the license plate and driver of every vehicle that enters.¹¹ A massive video surveillance system also watches the interior of the city.¹² Other British cities—according to one

8. GEORGE ORWELL, 1984 (1949). "George Orwell" was the pseudonym used by the English novelist and essayist Eric Blair.

9. Padgett, *supra* note 2, at 106.

10. Thus, the only reason that the main character of Padgett's story has no sense of privacy is that he is trying to get away with murder, and he knows that, once the killing occurs, police will have access to every segment of his life that might help them to prove that the killing was planned (rather than the accident he is trying to portray). *See id.*

11. MICHAEL MCCAILL & CLIVE NORRIS, CCTV IN LONDON 6 (Urban Eye, Working Paper No. 6, 2002), available at http://www.urbaneye.net/results/ue_wp6.pdf; Jeffrey Rosen, *A Watchful State: A Cautionary Tale for a New Age of Surveillance*, N.Y. TIMES MAG., Oct. 7, 2001, at 38, 41–42; *see also* Mark Townsend & Paul Harris, *Security Role for Traffic Cameras*, OBSERVER (London), Feb. 9, 2003 (discussing London's "ring of steel" and the use of facial recognition software), available at <http://www.guardian.co.uk/print/0,3858,4601963-111267,00.html>.

12. MCCAILL & NORRIS, *supra* note 11, at 6–16; Rosen, *supra* note 11, at 41–42; *see also* 48 *Hours: Lessons of Britain*, CBSNEWS.COM (Oct. 5, 2001) ("The people of Great Britain are the most watched in the world. Cameras are everywhere, watching nearly everything Across

count, at least 440 in all¹³—have also covered whole neighborhoods and business districts with cameras. American cities are rapidly following suit. Although most residents and visitors of New York remain oblivious to them, thousands of video cameras,¹⁴ many “indistinguishable from lampposts,” sit above parks and streets throughout the city and on the campuses of schools and universities.¹⁵ The City of Baltimore has installed cameras at “all 106 downtown intersections” and in its Inner Harbor area.¹⁶ The Washington, D.C. police department operates cameras that watch over downtown streets, subways, parks, and other public spaces and has plans to substantially expand its video surveillance system in the near future.¹⁷ Chicago has recently joined the list of major cities installing cameras over public streets,¹⁸ and other American cities are doing so as well.¹⁹

The cameras now proliferating in urban spaces are in many respects far more powerful than the video cameras of the past. Most can quickly pan, tilt, or rotate 360 degrees at the command of a far-away control room.²⁰ They can isolate an individual in a business district or subway station, zoom in on

Great Britain, there are more than two million surveillance cameras . . .”), at <http://www.cbsnews.com/stories/2001/10/04/48hours/main313586.shtml>.

13. Rosen, *supra* note 11, at 41.

14. Mark Boal, *The Surveillance Society: Part One: Spycam City*, VILLAGE VOICE (N.Y.), Sept. 30–Oct. 6, 1998, at 38, 40.

15. *Id.*; see also *Morning Edition: Profile: Use of Surveillance Cameras in New York City and Other Places Around the World* (NPR radio broadcast, Feb. 25, 2002) (noting reports of thousands of cameras in New York City and deliberations about installing “a hundred cameras with face recognition software in Times Square”), transcript available at 2002 WL 3187213.

16. DAVID BRIN, *THE TRANSPARENT SOCIETY: WILL TECHNOLOGY FORCE US TO CHOOSE BETWEEN PRIVACY AND FREEDOM?* 5 (1998); see also David A. Fahrenhold, *Crime-Plagued D.C. Neighborhoods Ask for Cameras*, WASH. POST, Mar. 10, 2003, at B1 (noting that Baltimore uses cameras to watch over its Inner Harbor area and the city’s east side).

17. See Jess Bravin, *Washington Police to Play ‘I Spy,’* WALL ST. J., Feb. 13, 2002, at B1 (noting that cameras in Washington, D.C. “already monitor mass-transit stations, monuments, and schools” and that plans are underway to extend the monitoring to “streets, shopping areas, and neighborhoods,” creating “what will soon be one of the nation’s most extensive public surveillance networks”); see also Fahrenhold, *supra* note 16 (noting that Washington, D.C. has “one of the most sophisticated police camera systems in the nation” and that the metropolitan police, United States Park Police force, and the United States Capitol Police use cameras to monitor public space in the city).

18. See David Heinzmann, *City to Put ‘Gotcha’ Cameras on Crime*, CHI. TRIB., July 11, 2003, at 1 (describing plans to put cameras atop light poles in areas where police want to disrupt drug traffic).

19. See Nikki Usher, *Video Surveillance Comes to the Big Easy*, SAN DIEGO UNION TRIB., Aug. 24, 2003, at A14 (listing twelve American cities using video surveillance); see also, e.g., *Richmond to Employ Surveillance Cameras*, DAILY PRESS (Richmond), Mar. 10, 2003, at C4 (describing the use of cameras in Richmond); Nikki Usher, *Who’s Watching You?*, TIMES-PICAYUNE (New Orleans), Aug. 9, 2003, at 01 (describing plans to install cameras throughout New Orleans).

20. See MARCUS NIETO ET AL., *PUBLIC AND PRIVATE APPLICATIONS OF VIDEO SURVEILLANCE AND BIOMETRIC TECHNOLOGIES* 4 (Cal. Research Bureau, CRB 02-006, Mar. 2002), available at <http://www.library.ca.gov/crb/02/06/02-006.pdf>.

him, and scrutinize facial expressions, movements, even reading materials in close detail.²¹ They often work not as isolated units, but as components of an integrated network of cameras that sends information from many different parts of the city back to a common observation center, which can then analyze the data as a whole or follow a person as he moves from one part of the city to another.²² The digitization of video images and tremendous expansions in computer memory have made it possible for operators to store substantial amounts of visual data and retrieve and search this data when they have a desire to view it.²³

In fact, the technology being developed today may one day go beyond the science fiction analogy. Detectives in Padgett's world had comprehensive records of images in video archives. Investigators in our own world have methods of connecting those images to identities and other information beyond what the camera shows. Using facial recognition software, investigators might quickly match a face to a specific name and then (with the aid of other databases) to that person's "medical history, tax records, criminal arrest records, voting records, political affiliations, and any other conceivable type of information."²⁴ Under such a surveillance regime, each life might become not merely an electronic "open book," but an "open web site," which investigators can use not only to rewind or fast-forward through large portions of a person's history, but to link to extensive data on (and perhaps visual recordings of) that person's colleagues, the organizations she belongs to, and various discussions or references regarding her that take place in her absence.²⁵

21. As Mark Boal notes, some of the cameras now available allow operators to "count the buttons on a blouse three miles away." Boal, *supra* note 14, at 40; *see also* NIETO ET AL., *supra* note 20, at 4 (noting that "many cameras are able to read a cigarette package label at a hundred meters").

22. The D.C. system, for example, is already linked in this way. The British system is not, but Jeffrey Rosen notes that "over the next few years, that seems likely to change, as Britain moves toward the kind of integrated Web-based surveillance system that Visionics [an American company manufacturing face recognition devices] has now proposed for American airports and subway systems." Rosen, *supra* note 11, at 43, 85.

23. *See* Nicholas Imparato, *Smart Cameras Get Ready for Prime-Time: For the Security Industry, It is Not So Much a Matter of Whether Smart Cameras Will Become a Mainstream Product, But When*, ADVANCED IMAGINING, Feb. 1, 2003, at S18 ("Camera costs are declining and bandwidth is increasing. Together with a decrease in the cost of processing power, they are loosening the physical restraints on making equipment ubiquitous."); *see also* GEN. ACCOUNTING OFFICE, VIDEO SURVEILLANCE: INFORMATION ON LAW ENFORCEMENT'S USE OF CLOSED CIRCUIT TELEVISION TO MONITOR SELECTED FEDERAL PROPERTY IN WASHINGTON, D.C. 5 (2003) [hereinafter GEN. ACCOUNTING OFFICE] ("Digital camera and storage technologies are rapidly replacing traditional analog systems."), available at <http://www.gao.gov/new.items/d03748.pdf>.

24. Joyce W. Luk, *Identifying Terrorists: Privacy Rights in the United States and the United Kingdom*, 25 HASTINGS INT'L & COMP. L. REV. 223, 230 (2002).

25. As Vance Bjorn writes, "[w]ith computer vision techniques it will not be long before this stream of unstructured data [caught on video surveillance cameras] is automatically reduced to a

To be sure, the increasing use of cameras and facial recognition software does not by itself condemn us to live in a world where our pasts can be “traced” by curious officials. The vast majority of images captured by these cameras are likely to receive little scrutiny from the necessarily limited staff that operates them, and most images they do register are likely to be forgotten soon afterwards.²⁶ Facial recognition technology likewise must overcome significant hurdles before it can function as an effective mechanism for instantly tracking and identifying people in public streets.²⁷ But technological developments are rapidly transforming camera systems and facial recognition devices into far more powerful instruments than they once were.²⁸ Although we do not yet live in Padgett’s world, “[o]ne need not be a science fiction fan,” as mapping expert Mark Monmonier points out, “to envision a future in which cameras as dense as streetlights feed images to central computers with face-recognition algorithms and biometrics software that match pedestrians to their stored profiles and track their movement through streets and parks.”²⁹

running commentary of who, what, where, and why of the activities and people caught on tape.” See Vance C. Bjorn, *An Introduction to Privacy and Security Considerations of Biometrics Technology*, in *THIRD ANNUAL INSTITUTE ON PRIVACY LAW: STRATEGIES FOR LEGAL COMPLIANCE IN A HIGH TECH & CHANGING REGULATORY ENVIRONMENT* 105, 109 (PLI Patents, Copyrights, Trademarks, and Literary Property Course Handbook Series No. 701, 2002). As one developer of face recognition technology notes, a search of particular faces within a database of images functions “much like a Google search.” See Lee M. Webb, *Imagis Technologies Inc.—Imagis Nabs TV Face Time, Broker Ally Makes Other News*, CAN. STOCKWATCH, June 26, 2002, at <http://www.stockwatch.com>.

26. See Clive Norris et al., *Algorithmic Surveillance: The Future of Automated Visual Surveillance*, in *SURVEILLANCE, CLOSED CIRCUIT TELEVISION, AND SOCIAL CONTROL* 255, 256–57 (Clive Norris et al. eds., 1998) (stating that the “exponential increase in visual surveillance creates a massive and costly problem of information processing and handling” and that “human monitoring is still very limited”).

27. See Nicholas Orlans, *Facial and Voice Recognition*, in JOHN D. WOODWARD, JR. ET AL., *BIOMETRICS: IDENTITY ASSURANCE IN THE INFORMATION AGE* 71, 74 (2003) (stating that “[e]ven with additional years of refinements and improvements [after the research and testing of the 1980s and the 1990s] today’s techniques work best under controlled environmental conditions” and that “when crowd conditions are considered . . . performance degrades”); P. Jonathon Phillips et al., *Face Recognition Vendor Test 2002: Overview and Summary* 14 (Mar. 2003) (concluding that “[o]utdoor face recognition performance needs improvement”), at http://www.frvt.org/DLs/FRVT_2002_Overview_and_Summary.pdf.

28. See Norris et al., *supra* note 26, at 266–68 (noting that in spite of current problems hindering the use of facial recognition for public surveillance, it is “now technologically feasible to imagine that, in some not too distant future, as we walk down the city streets we will not only be photographed, but automatically identified as well”); see also *infra* subpart III(A).

29. MARK S. MONMONIER, *SPYING WITH MAPS: SURVEILLANCE TECHNOLOGIES AND THE FUTURE OF PRIVACY* 115 (2002); see also JEFFREY ROSEN, *THE NAKED CROWD: RECLAIMING SECURITY AND FREEDOM IN AN ANXIOUS AGE* 45–46 (2004) (“Once thousands of cameras from hundreds of separate CCTV systems are able to feed their digital images to a central monitoring station, and the images can be analyzed with face- and behavioral-recognition software to identify unusual patterns, then the possibilities of the Panopticon will suddenly become very real.”). Indeed,

Paradoxically, the part of Padgett's imagined world that fits least comfortably into the emerging landscape of twenty-first century government surveillance is the part that would probably strike Fourth Amendment scholars as the most familiar: the rule that visual records of our lives can be accessed only for purposes of investigating a "serious crime."³⁰ This is not because there is anything obviously unreasonable about requiring government officials wishing to page through an individual's past first to request a warrant based on probable cause that such an intrusive investigation will uncover evidence of criminal activity. On the contrary, there are good reasons to think that our legal regime should interpose a warrant requirement, or some equivalent legal hurdle, between government authorities and video records of its citizens' day-to-day lives.

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."³¹ Police must obtain a warrant from a neutral magistrate before they can engage in technologically-primitive searches of an individual's journals, letters, and other evidence of past activities.³² It would be odd to place no such restrictions on their ability to view a more comprehensive and vivid record of a person's history in a video database.³³

even if face recognition systems themselves develop more slowly than authorities hope, video camera systems might use other surveillance technologies to match names (and other information) to pictures: they might use cell phone records, electronic records of drivers' movements, or other biometric data one leaves in public places to figure out who they are watching on a camera screen or video tape.

30. See Padgett, *supra* note 2, at 106.

31. U.S. CONST. amend. IV.

32. The search of private papers was the central focus of both *Entick* and *Wilkes*, two of the search and seizure cases that led the founders to arm citizens with a right against "unreasonable searches." See *Boyd v. United States*, 116 U.S. 616, 625–26 (1885) (describing *Entick v. Carrington*, 95 Eng. Rep. 807 (K.B. 1765), and *Wilkes v. Wood*, 98 Eng. Rep. 489 (K.B. 1763), as "fresh in the memories of those who . . . established our form of government"). As the Supreme Court stated in *Boyd*, these cases emphasize the importance of protecting "private papers" from arbitrary government examination. See *id.* at 627–28 (citing Lord Camden's statement in *Entick* that "[p]apers are the owner's goods and chattels; they are his dearest property, and are so far from enduring a seizure, that they will hardly bear an inspection").

33. One might object that journals, letters, and other private papers are likely to contain confidential information of a sort one rarely finds in videos of public interactions: namely, descriptions of thoughts and feelings. But individuals can and sometimes do discuss or display private thoughts or feelings with friends or family in public, at least when they are in an environment where they are secluded or no one is likely to be listening. Even the silent video surveillance of the kind now used in most cities might soon be able to let observers read lips or discern much from examining facial expressions. Moreover, even where a document in a person's drawer does nothing more than describe events in the outside world, police still need a warrant to open the drawer and read it. It is unlikely that this requirement is only because judges worry about the possibility that the police will find a record of thoughts and feelings—a description of day-to-day events may also be private.

Indeed, the absence of some such constitutional limitation seems to leave authorities free to engage in a variant of the dragnet searches that the Fourth Amendment was clearly intended to prevent. The drafters of the Bill of Rights gave individuals protection against “unreasonable searches and seizures” in order to assure that people walking down a street, for example, could not be stopped randomly and searched by a government official who had no reason to suspect them of wrongdoing. With comprehensive video archives, authorities would again 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 silent and invisible searches by far-away camera operators do not limit a person’s physical movement³⁴ or subject him to the kind of unsettling physical intrusion that occurs when a police officer stops and frisks him in the street. But the sense that one is at all times subject to close monitoring can be just as unsettling as a brief on-site search. Unlike the individual who is freed from intensive scrutiny after a police frisk, an individual walking through streets laden with cameras can never be sure that the monitoring has ended.³⁵

It would not be surprising, therefore, if courts sought to ensure that such powerful electronic personal searches took place only within constitutional boundaries as strict as those which confine their (more spatially and temporally limited) physical counterparts—perhaps only, as Padgett suggested, when authorities have probable cause to believe that searching a particular person or place is necessary to investigate a “serious crime.”³⁶

34. For this reason, they are highly unlikely to constitute a “seizure” under the Fourth Amendment, because “a person has been ‘seized’ within the meaning of the Fourth Amendment only if, in view of all of the circumstances surrounding the incident, a reasonable person would have believed that he was not free to leave.” *United States v. Mendenhall*, 446 U.S. 544, 554 (1980). Some courts have concluded that videotaping can constitute a Fourth Amendment seizure of an intangible possession. *See, e.g., Caldarola v. County of Westchester*, 343 F.3d 570, 574 (2d Cir. 2003) (holding that “the making of [a] videotape resulted in the seizure of [the defendant’s] image” and thereby implicated Fourth Amendment interests). Such an argument seems implausible, since it would treat every photograph of a person by public authorities as implicating Fourth Amendment interests. For this reason, my focus in this Article is on whether videotaping can constitute a Fourth Amendment search.

35. As a number of commentators have noted, searches by far-away camera operators may be even more intrusive in one respect than on-site physical searches because an unobserved camera operator is less likely than a police officer acting in full view of others to have qualms about scrutinizing people in ways that conflict with widespread social norms. As Sherry Colb notes, “you can’t stare back to discourage the privacy intrusion.” Molly Smithsimon, *Private Lives, Public Spaces*, *DISSENT*, Winter 2003, at 43, 44 (paraphrasing Colb); *see also infra* subpart III(B).

36. Padgett, *supra* note 2, at 106.

But while such constitutional limits on wide-scale video surveillance may seem intuitively reasonable and necessary, contemporary Fourth Amendment jurisprudence is ill-equipped to provide or even delineate them for at least two reasons. The first is that mass video surveillance occurs in the public realm—in streets, parks, and highways—where courts have been reluctant to find that individuals have reasonable expectations of privacy, at least in that information which they fail to conceal.³⁷ Unlike random stops and searches by government officials, extensive video surveillance does not dig beneath the visible surface that people project to the world.

As a consequence, contemporary Fourth Amendment jurisprudence differentiates pervasive video surveillance from more familiar mass suspicionless searches in one crucial respect: by holding that it is not a “search” at all.³⁸ Fourth Amendment “searches,” according to the Supreme Court’s current test, do not include all investigations of the sort an English speaker might describe as a “search.”³⁹ As the Supreme Court emphasized in its landmark decision in *Katz v. United States*, which still provides the key legal test for what counts as a “search,” “what a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection.”⁴⁰ Thus, even when police carefully scan a crowd with binoculars, in search of a particular person, they are not engaging in a *Fourth Amendment* “search.”⁴¹ Fourth Amendment interests are implicated only when the government uncovers things that people conceal. Because the Fourth Amendment offers protection only against suspicionless searches and seizures—and not against suspicionless examinations (no matter how rigorous)—public camera networks would seem to be outside of the Fourth Amendment’s ambit, at least as long as their focus remains on public space and does not wander into private homes, offices, or other enclosed areas.⁴²

In the context of mass video surveillance, however, this is a strange result. Even a video archive that includes only a person’s movements

37. *Katz v. United States*, 389 U.S. 347, 351–52 (1967).

38. Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 236 n.106 (2002) (listing fourteen cases that hold that public surveillance is not a search because any expectation of privacy would be unreasonable).

39. *Id.*

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

41. See *infra* section II(B)(2) (citing cases where courts found that the use of magnification to view public activity was not a search).

42. One might argue that even if video surveillance were to constitute a “search,” it would not be a search of “persons, houses, effects, and papers,” which are the only kinds of searches that the Fourth Amendment covers. But most video surveillance is used to capture images of persons that potentially reveal more information about them than would be revealed in a pat-down search by a police officer. And video surveillance that reveals details of people’s reading materials or possessions might also count as a search of “effects” or “papers.”

through public settings would inevitably reveal much that he would rather not share with an audience, let alone have incorporated into official records. A person usually cannot enter a psychiatrist's office, marriage counseling center, or infertility clinic except from a public street. It is often in public that people ask others out on a date, join a religious community, or seek resources in a library for educating themselves about medical concerns or social dilemmas. Of course, even in these deeply personal aspects of our public lives, there is at least a small chance we will be photographed or filmed by others nearby. But such third parties are unlikely to know when we will be there or who we are, and they will usually go away with only a brief snapshot of our lives. By contrast, a government agency armed with a comprehensive visual record of our public activities would not have to guess when we might reveal personal information in public, as it could probe our lives after the fact, and might quickly build a more complete picture (for example, figuring out what specific medical or social problem led us to a certain source of help) by looking elsewhere in its substantial database of the recorded images and other information that we leave behind as we move through visually-surveilled public space.

Moreover, making so much of our day-to-day lives available for display intuitively constitutes a much more significant intrusion into our privacy than many briefer and more limited examinations that courts have not hesitated to classify as "searches." The Supreme Court has given force to Fourth Amendment protections, for example, where a principal looks through a student's purse.⁴³ Students "may find it necessary to carry with them a variety of legitimate, noncontraband items," said the Court, "and there is no reason to conclude that they have necessarily waived all rights to privacy in such items merely by bringing them onto school grounds."⁴⁴ Reviewing a roadblock program on public highways, the Court likewise emphasized that "people are not shorn of all Fourth Amendment protection when they step from their homes onto the public sidewalks. Nor are they shorn of those interests when they step from the sidewalks into their automobiles."⁴⁵

In the above cases, the Court discussed things or acts hidden from the rest of the world in a car or a container. But the same logic applies with equal force to the activities captured by public cameras: it is difficult (if not impossible) for individuals to avoid providing significant evidence of

43. *New Jersey v. T.L.O.*, 469 U.S. 325, 333 (1985).

44. *Id.* at 339. The Court ultimately decided that the school principal did not need a warrant to conduct a search because, given the circumstances, a warrantless search was reasonable. *Id.* at 340–

41. However, the Court did not exempt the search of the purse from the scope of the Fourth Amendment. *Id.* at 336–37.

45. *Delaware v. Prouse*, 440 U.S. 648, 663 (1979) (citation omitted).

thoughts and personal interests as they walk on a public street—through their facial expressions, interactions with others, and choices of activities. A detective or spy wishing to build a dossier on an individual's life and personality would probably learn more from examining a searchable database of such images than he would by rummaging through a purse, wallet, or suitcase, especially if he could link from the images to other information about the individual's identity and background. Yet contemporary Fourth Amendment jurisprudence seems to provide protection only against the lesser of these intrusions. Indeed, while public surveillance video systems were first used in the 1960s⁴⁶ and are becoming more prevalent, federal courts have yet to seriously address the question of how to analyze them under the Fourth Amendment.⁴⁷

When they do, they will find there is a second reason—apart from the “surface-bound” nature of such surveillance and its focus on open places—that contemporary Fourth Amendment doctrine may fail to give force to the probable cause protections that Lewis Padgett imagined would keep powerful video surveillance technology in check.⁴⁸ The Fourth Amendment does not bar all warrantless searches; it bars only those that are unreasonable.⁴⁹ Even if public video surveillance is a search under the Fourth Amendment, one might argue that it is nonetheless reasonable even when left unconstrained by warrant and probable cause requirements. Such arguments have been most likely to gain support when the crime the government investigators are working to prevent is an act of terrorism.⁵⁰ Many ordinary would-be criminals might be deterred from theft or violent crime simply by the prospect that the police will be able to easily identify them after the fact (although the evidence for the deterrent powers of existing surveillance systems is by no means clear).⁵¹ By contrast, suicide bombers are much harder to detect and deter. They are often unintimidated by the prospect of being identified in the aftermath of a bombing and are likely to have done all the damage they want to do—in the form of massive loss of human life and massive damage to individuals' sense of security—before police even begin their investigation. To fight terrorism effectively, one might argue, authorities must closely scrutinize numerous people before they have probable cause for focusing on one person or another, just as airports trying to prevent

46. See *infra* note 179 and accompanying text.

47. See *infra* subpart II(A).

48. Padgett, *supra* note 2, at 106.

49. U.S. CONST. amend. IV.

50. See Lisa Guernsey, *Living Under an Electronic Eye*, N.Y. TIMES, Sept. 27, 2001, at G1 (describing public opinion polls taken shortly after September 11, 2001).

51. See *infra* section V(B)(2).

hijackings examine all passengers and all luggage instead of trying to narrow their search for terrorists on the basis of insufficient information.⁵²

In the past, courts have recognized that the need to avoid such devastating loss of life demands flexibility in interpreting search and seizure requirements and sometimes requires allowing authorities to conduct searches without any “individualized suspicion” of wrongdoing.⁵³ As Justice O’Connor recently noted, courts have been more willing to dispense with individualized suspicion requirements when “even one undetected instance of wrongdoing could have injurious consequences for a great number of people.”⁵⁴ For example, “fires and epidemics [that] ravage large urban areas,”⁵⁵ train wrecks that cause “great human loss,”⁵⁶ and plane hijackings that claim “hundreds of human lives”⁵⁷ are less likely to require these individualized requirements. The threat of terrorism seems to provide just as compelling of a reason to lift warrant and probable cause requirements that might slow the use of public video surveillance to gather (and track) leads needed to uncover and prevent planned terror attacks.

But the battle against terrorism does not easily fit into the model created by courts to deal with the safety threats they addressed in the latter decades of the twentieth century. The searches used by the government to address each of the threats described above were brief and confined to a certain facet of life: weapon checks that take place only at airports,⁵⁸ periodic and limited housing inspections,⁵⁹ and brief alcohol and drug tests aimed exclusively at train operators or other employees whose jobs had potentially significant implications for public safety.⁶⁰ Unlike the threats such searches are meant to detect, the threat posed by terrorism is designed to create, and often does create, a fear of sudden and devastating loss that is not confined to a limited

52. See *United States v. Moreno*, 475 F.2d 44, 49 (5th Cir. 1973) (“Obviously, in order to jeopardize the lives and safety of the smallest number of people, the hijacker must be discovered when he is least dangerous to others and when he least expects confrontation with the police. In practical terms, this means while he is still on the ground and before he has taken any overt action.”). See generally WAYNE R. LAFAYE, *SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT* § 10.6 (3d ed. 1996) (outlining the history and legal implications of airport searches).

53. See *City of Indianapolis v. Edmond*, 531 U.S. 32, 44 (2000) (noting that an “imminent terrorist attack” is sufficient cause to allow authorities to conduct an otherwise impermissible roadblock).

54. *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 675 (1995) (O’Connor, J., dissenting).

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

56. *Skinner v. Ry. Labor Executives’ Ass’n*, 489 U.S. 602, 628 (1989).

57. *United States v. Edwards*, 498 F.2d 496, 500 (2d Cir. 1974) (quoting *United States v. Bell*, 464 F.2d 667, 675 (2d Cir. 1972) (Friendly, J., concurring)).

58. *Id.* at 501–02.

59. *Camara*, 387 U.S. at 535.

60. *Skinner*, 489 U.S. at 628.

portion of our day-to-day existence, but instead permeates the whole of public life.⁶¹ This widespread threat was made clear by the variety of settings and possible scenarios that were the subject of terrorist warnings in the months after September 11, 2001. The government warned that explosives might be used in malls, bridges, apartments, and trains;⁶² that scuba-diving terrorists might sabotage boats or strike coastal areas;⁶³ that attackers might use trucks or other vehicles as weapons on public roadways;⁶⁴ and that they might poison water supplies,⁶⁵ target large holiday gatherings⁶⁶ and national monuments,⁶⁷ shoot down airplanes with missiles,⁶⁸ or use explosives, chemical weapons or radiological bombs to kill thousands in subways or town centers.⁶⁹ The variety and unpredictability of possible attacks, in method and location, has made some authorities despair of

61. As William Stuntz has noted, terrorist attacks are harder to prevent than street crimes because “[t]hey are too geographically dispersed, and the attackers are too sophisticated—this is not opportunistic crime in a few ‘hot spots,’ but something both less visible and less easily deterred. To find and prevent it, the police need information.” William J. Stuntz, *Local Policing After the Terror*, 111 YALE L.J. 2137, 2161 (2002).

62. Bob Miller & Christine Haughney, *Nation Left Jittery by Latest Series of Terror Warnings*, WASH. POST, May 22, 2002, at A01, available at <http://www.washingtonpost.com/ac2/wp-dyn/A51195-2002May21?html>; see also Summary of ERRI Terrorist Alerts/Advisories—1998–2003 [hereinafter ERRI Terrorist Advisories] (mentioning intelligence suggesting possible attacks on malls or banks in April of 2002, a May 2002 alert that Al Qaeda operatives might rent apartments and use them to bomb apartment complexes, and a February 2003 alert that Al Qaeda might target hotels), at <http://www.emergency.com/2001/ter-advrsry-sum.htm> (last visited Mar. 21, 2004).

63. *Terrorists May Use Scuba Divers, Planes*, ABCNEWS.COM (May 24, 2002), at <http://abcnews.go.com/sections/us/dailynews/homefront0020524.html>; see also ERRI Terrorist Advisories, *supra* note 62 (describing a May 2002 FBI warning that “various terrorist elements have sought to develop an offensive scuba diver capability” and a June 2002 alert indicating plans to use “low-profile kayaks, packed with explosives, for an [sic] possible assault on ships or waterfront facilities”).

64. See ERRI Terrorist Advisories, *supra* note 62 (describing a June 2002 FBI warning that terrorists might use fuel tankers, particularly in attacks on Jewish neighborhoods).

65. Neil Johnson, *Water Utilities Tighten Security at FBI's Urging*, TAMPA BAY ONLINE, Sept. 27, 2001, at <http://news.tbo.com/news/MGAUYAT24SC.html>.

66. See ERRI Terrorist Advisories, *supra* note 62 (warning in January 2002 of a possible attack on the Winter Olympics in Salt Lake City and in June 2002 of a possible attack on the Fourth of July).

67. See *id.* (describing a warning announced in May and September 2002 suggesting possible attacks on the Brooklyn Bridge, the Statue of Liberty, and other landmarks).

68. See *id.* (warning in January 2003 of an increasing threat that heat-seeking missiles will be used to shoot down airplanes).

69. See *id.* (noting a May 2002 “warning about possible terrorist attacks on rail and transit systems across the nation,” an FBI warning in June 2002 concerning a “potential nerve gas attack against subway systems” in the United States, a warning in October 2002 suggesting attacks on the rail system, and an announcement made in February 2003 that “al-Qaeda and other terrorist groups might try to use chemical, biological or radiological weapons such as a ‘dirty bomb’”).

countering them except by suspicionless surveillance techniques that stretch across all of public life, and capture all manner of detail.⁷⁰

But such a proposal is troubling because even if advanced surveillance technologies showed great promise in countering terrorism,⁷¹ unconstrained and pervasive camera networks would protect the public sphere only by changing its character. The use of such technologies might lessen anxiety about violence in public spaces, but it would do so by undermining the forms of freedom that people traditionally seek (and find) in these spaces.⁷² Generally, the Supreme Court has allowed generalized suspicionless surveillance only in environments such as workplaces, schools, and high security zones, where people are already subject to a substantial degree of oversight and constraint.⁷³ Even in these situations, it has imposed constitutional limits on the scope of such searches to ensure against abuses of discretion.⁷⁴ Individuals who have to be self-conscious in such controlled environments have been able to find a refuge in other public settings—parks, streets, public squares—for freer and more spontaneous behavior, something they could hardly do if such settings were under a scrutiny even more sustained and extensive than that the courts have allowed in highly-regulated environments.⁷⁵

70. See ROSEN, *supra* note 29, at 33–34 (noting that because people believe “[a] terrorist could be lurking on any corner in America,” people have recommended comprehensive video surveillance schemes, such as “the installation of 100 biometric surveillance cameras in Times Square” and numerous other public areas); see also *id.* at 56 (noting that the person in charge of developing Washington, D.C.’s emerging camera system has said that “[i]n the context of September 11, we have no choice but to accept greater use of this technology,” and that he was “intrigued” by the British model of surveillance).

71. As noted in Part IV, there is little evidence that existing systems are effective in thwarting either terrorism or other kinds of violent crime.

72. As Walter Gellhorn has noted, in a passage quoted recently in a dissent by a Canadian Supreme Court Justice, “[r]estrictions justified as necessary safeguards of freedom may in fact safeguard freedom out of existence altogether.” WALTER GELLHORN, *INDIVIDUAL FREEDOM AND GOVERNMENTAL RESTRAINTS* 40 (1956), *quoted in* R. v. Landry, [1986] S.C.R. 145, 188 (La Forest, J., dissenting).

73. See, e.g., *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 655 (1995) (“[A] proper educational environment requires close supervision of schoolchildren, as well as the enforcement of rules against conduct that would be perfectly permissible if undertaken by an adult.” (quoting *New Jersey v. T.L.O.*, 469 U.S. 325, 339 (1985))); *Skinner v. Ry. Labor Executives’ Ass’n*, 489 U.S. 602, 627 (1988) (noting that “the expectations of privacy of [railroad employees covered by drug testing requirements] are diminished by reason of their participation in an industry that is regulated pervasively”).

74. See *T.L.O.*, 469 U.S. at 342–43 (refusing to “authorize unrestrained intrusions upon the privacy of schoolchildren” and requiring reasonableness in searches under the circumstances).

75. *Skinner*, 489 U.S. at 624 (permitting searches without individualized suspicion when privacy interests are minimal and governmental interests would be frustrated by requiring individualized suspicion).

This lack of fit between existing jurisprudence on the one hand and emerging threats to privacy and security on the other hand requires a novel analysis of search and seizure protections. Even the significant constitutional thinking that courts have engaged in to fit the Fourth Amendment to twentieth-century developments—new electronic surveillance technologies and security threats distinctive to modern life—needs rethinking if constitutional privacy protections are to work well in twenty-first century conditions. In particular, courts have to think carefully about how to give Fourth Amendment protections greater force in the public sphere.

How can courts extend constitutional privacy protection to open and observable activities in spite of long-standing judicial reluctance to do so? One might suggest that the starting point for an answer lies in strongly reaffirming one of the most widely-repeated statements in the Supreme Court's influential decision in *Katz v. United States*: "[T]he Fourth Amendment protects *people not places*."⁷⁶ After all, one of the key arguments against extending constitutional limits to public camera systems is that the sidewalks, parks, and plazas that these camcras watch over are not private places like the home.⁷⁷ The best way to respond to this claim, one might argue, is to stress that the Fourth Amendment does not protect the privacy of places, but the privacy of *the people* in these places, and its protections can move *with* people as they leave their homes and move from place to place, taking private information with them.⁷⁸ One can restate this point in the language that Justice Harlan proposed in his concurring opinion in *Katz*, which the Court has since adopted as its test for what constitutes a "search."⁷⁹ The Fourth Amendment, one might say, protects privacy *anywhere* that people *reasonably expect* to have such privacy.⁸⁰ Since people reasonably expect to be free from ongoing government surveillance even on sidewalks, plazas, and parks, the Fourth Amendment should have force in

76. *Katz v. United States*, 389 U.S. 347, 351 (1967) (emphasis added).

77. See, e.g., *Richmond to Employ Surveillance Cameras*, *supra* note 19 (describing the installation of video cameras in Richmond streets and quoting the Richmond Police Chief's statement that "we monitor spaces where there's no Constitutional right to privacy," and reporting that even the ACLU director in Richmond conceded that "[i]t's pretty clear that it is not unconstitutional to place cameras in public places"); Susan McCoy, Comment, *O'Big Brother Where Art Thou?: The Constitutional Use of Facial-Recognition Technology*, 20 J. MARSHALL J. COMPUTER & INFO. L. 471, 485 (2002) (noting that "[n]o individual can reasonably expect to maintain privacy in a public forum").

78. See *infra* Parts I and IV for cases elaborating on this view.

79. See, e.g., *California v. Ciraolo*, 476 U.S. 207, 211 (1986) ("The touchstone of Fourth Amendment analysis is whether a person has a 'constitutionally protected reasonable expectation of privacy.'" (quoting *Katz*, 389 U.S. at 360 (Harlan, J., concurring))).

80. See *Katz*, 389 U.S. at 360 (Harlan, J., concurring) (explaining that a home and a telephone booth, unlike a field, are areas that a person would have a "constitutionally protected reasonable expectation of privacy").

these public environments as well as in the home or office and should allow for monitoring of public life only to the extent needed to prevent terrorism or serious crime. This kind of justification is offered by certain powerful critiques of unconstrained public video surveillance. For example, a former justice of the Canadian Supreme Court advised that, under his country's analogue of the Fourth Amendment, courts should dispense with "rigid, formalistic borders between private and public spatial domains" and instead attend to what constitutes a "reasonable expectation of privacy in a given context."⁸¹ Christopher Slobogin has likewise built a compelling case for constitutional restriction of public video surveillance by "tak[ing] seriously the Court's admonition that the Fourth Amendment's scope is ultimately defined by 'expectations of privacy society is prepared to recognize as reasonable.'"⁸²

This Article, however, will suggest that a different approach provides a more promising foundation for modern Fourth Amendment jurisprudence. It will argue that, contrary to *Katz*'s famous pronouncement, courts can often best protect privacy in public life by focusing on *places* rather than the people who act in them. Instead of protecting individual expectations of privacy directly, courts might best protect privacy in public life *indirectly* by identifying and protecting those features of our society, including those features of public space, that allow anonymity and other privacy-related interests to exist in sufficient measure. This approach better captures what is disturbing about widespread public video surveillance. Such surveillance threatens Fourth Amendment values not simply through its effects on the privacy of any individual activity, but by wholly transforming the public environment in a way that is at odds with core requirements of a free society. This approach is also more helpful than the *Katz* framework in clarifying the core of the challenge that confronts us as we adapt Fourth Amendment protections to the threats posed by terrorism and other violent crime. This challenge is not to freeze and give force to every existing expectation of privacy that individuals might have had before confronted with such threats. Nor is it to make Fourth Amendment protections fluctuate with Americans' changing (and heterogeneous) preferences about privacy. It is rather to assure that, even as courts allow government officials to hunt more vigorously for evidence of criminal activity or signs of terrorist threats, and

81. Letter from Justice Gérard La Forest, former Canadian Supreme Court Justice, to George Radwanski, Privacy Commissioner of Canada, at notes 22–24 and accompanying text (Apr. 5, 2002), at http://www.privcom.gc.ca/media/nr-c/opinion_020410_e.asp.

82. Slobogin, *supra* note 38, at 271. Slobogin also explores the possibility that video surveillance might be restricted by other constitutional provisions, such as First Amendment protections of anonymity and the freedom of movement and informational privacy rights rooted in the Fourteenth Amendment. *Id.* at 252–67.

use new technologies to do so, they do not compromise those core privacy protections that are integral to a free society.

To be sure, *Katz*'s "reasonable expectation of privacy" test has not been without value in protecting privacy in the face of previous technologically-driven transformations of our environment. It created a useful framework for analyzing bugging, wiretapping, thermal imaging, and other techniques that allow investigators outside of a home, office, or phone booth to somehow look or hear inside. However, this framework is not as useful for analyzing emerging video surveillance systems, which invade our privacy by continuously gathering and analyzing the significant evidence of our thoughts, interests, and actions that we leave in the "outside" world itself.

Part I looks more closely at the development of the *Katz* test and considers why, although the *Katz* majority set out to provide a framework that would protect privacy "even in an area accessible to the public,"⁸³ its protections actually extended only to spaces that were in some sense enclosed or marked off by clear boundaries from the outside world (for example, homes, phone booths, and perhaps "virtual spaces" for electronic communications).

Part II explains how recent technological developments—particularly in video surveillance, tracking technology, and biometric identification—have allowed officials to circumvent *Katz*'s protection of private environments by collecting significant information about us that we inevitably leave behind as we move through public space. While courts have not squarely confronted this difficulty, some courts have noted it and expressed the sense that it may require somehow extending Fourth Amendment protections even to activity that is already open to public view.

Part III proposes a solution to this problem. Just as the Supreme Court after *Katz* (and most notably in *Kyllo*)⁸⁴ barred governments from simply circumventing (or eroding) the privacy-protecting features of houses and other traditionally private environments, twenty-first century courts should similarly bar government from technologically nullifying the privacy-protecting features of public space. As this part explains, such a focus on protecting the public environment has an important advantage over *Katz*'s "reasonable expectations test." It frees courts from the burden of making controversial judgments about what kinds of individual activities are sufficiently "intimate" to deserve Fourth Amendment protection. Having fortified the features of both private and public environments that make unmonitored activity possible, courts can leave individuals to decide for

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

84. *Kyllo v. United States*, 533 U.S. 27, 32 (2001).

themselves what legally permissible activities they would like shielded from observation by others. I also explain here why this task—the task of preserving an environment that is suitable for privacy and liberty—should be a matter of constitutional law, and not only a job for legislators. Although this judicial imperative will necessarily place some limits on the uses majorities make of new surveillance technologies, it need not cast courts in the role of Luddites, bent on denying police valuable crime-fighting technologies that many others (including perhaps criminals) are left free to use. A sound Fourth Amendment jurisprudence for public space would let law enforcement agents make extensive use of new technologies so long as protections for privacy interests are built into the technology itself or provided by a warrant or warrant substitute, which ensures that such technologies are used narrowly for proper ends.

Having examined more closely what this alternative to the *Katz* test entails, Part IV of the Article then asks whether this approach for replacing *Katz*'s reasonable expectations test is really superior to a revised "reasonable expectations" approach—one that explains why people might in fact reasonably expect protection against unconstrained video surveillance even in public. Although the language of reasonable expectations certainly allows room for a vigorous defense of "public privacy," its ambiguity blurs the clear lines people often depend on to figure out where and when they are free from monitoring and leads courts to confuse situations where privacy interests are absent with very different situations where privacy interests must share space with other important public interests, but deserve vigorous protection at the same time.

Finally, Part V examines the question of when it is reasonable for police or other government officials to use public video surveillance even though it is a search. It argues that while the devastation and unpredictability of terrorism may make virtually every search in public seem a reasonable and necessary one, the need to protect the character of the public sphere requires courts to insist, whenever possible, on statutory, programmatic, or technological constraints that will make video searches as safe as possible for the freedom from government scrutiny that people have traditionally found in streets, parks, and other public spaces.

1. The *Katz* Revolution: Strengthening and Expanding the Protection of Private Spaces

Science fiction writers are not the only ones who have imagined a world where all forms of individual privacy might be erased by futuristic technologies. In 1928, Justice Louis Brandeis noted that "[i]n the application

of a constitution . . . our contemplation cannot be only of what has been but of what may be”⁸⁵ and went on to describe “what may be.” He imagined various threats that scientific advances might one day pose to Fourth Amendment protections: the possibility that “without removing papers from secret drawers,” officers might somehow “reproduce them in court” and that “advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions.”⁸⁶

Brandeis’s purpose in painting this picture of future technology was to show that the Fourth Amendment interpretation of many of his Supreme Court colleagues—an interpretation which equated “searches” only with physical intrusions into a person’s home or property—would leave the home and all other centers of privacy entirely unprotected against numerous “[s]ubtler and more far-reaching means of invading privacy [that] have become available to the Government.”⁸⁷ The occasion for this warning was the case of *Olmstead v. United States*, which addressed the question of whether police officials violated the Fourth Amendment’s prohibition against “unreasonable searches” when they intercepted and listened to the defendant’s phone calls.⁸⁸ Unlike Brandeis, the Court’s majority (in an opinion by Chief Justice Taft) found that such wiretapping did not violate or even implicate the Constitution.⁸⁹ Indeed, the Court not only rejected the defendant’s claim that the government’s wiretapping was an “unreasonable search,” it found that there was no “search” at all.⁹⁰ “There was no entry of the houses or offices of the defendants” and the government could therefore not be viewed as overstepping any constitutional boundary lines.⁹¹ The defendant’s phone lines were “not part of [the defendant’s] house or office any more than are the highways along which they are stretched.”⁹² And no one could reasonably expect Fourth Amendment protection against official scrutiny when he “installs in his house a telephone instrument with connecting wires intend[ing] to project his voice to those *quite outside*.”⁹³ Messages projected to the world outside the home might be heard by those outside the home and, as the Court noted, the police had secured information from the suspect’s conversations “by the use of the sense of hearing and that only.”⁹⁴ It would be perverse, the Court emphasized, to place any constitu-

85. *Olmstead v. United States*, 277 U.S. 438, 473 (1928) (Brandeis, J., dissenting).

86. *Id.* at 474.

87. *Id.* at 473.

88. *Id.* at 456–57.

89. *Id.* at 466.

90. *Id.*

91. *Id.* at 464.

92. *Id.* at 465.

93. *Id.* at 466 (emphasis added).

94. *Id.* at 464.

tional hurdles before officials wishing to listen to sounds that are available to them. The meaning of searches and seizures, said Chief Justice Taft, may not be so enlarged as to “forbid hearing or sight.”⁹⁵

For Brandeis, such a view was appropriate only for previous times, when officials interested in seizing a person’s “papers and other articles incident to his private life” could do so only by “breaking and entry.”⁹⁶ To prevent such invasions, courts simply had to stop the physical acts that made them possible. But with modern technologies such as wiretapping, police officials could get much of a person’s private information even while remaining outside the home. Rather than guarding only against physical invasions, argued Brandeis, the Fourth Amendment must protect against “every unjustifiable intrusion by the Government upon the privacy of the individual.”⁹⁷

While Brandeis lost this specific battle, his insistence that courts must fortify the Fourth Amendment against new technologies was ultimately heeded by the Court. In the 1967 case of *Berger v. New York*, the Court rejected *Olmstead*’s conclusion that Fourth Amendment protections could not extend to wiretapping.⁹⁸ Later that year, it expressly overruled *Olmstead*’s “physical trespass” interpretation of the Fourth Amendment in *Katz v. United States*.⁹⁹ On the surface, the *Katz* decision may appear to be a fundamental shift in Fourth Amendment jurisprudence. Before *Katz*, the Fourth Amendment protected against search and seizure simply by safeguarding certain constitutionally protected areas, most notably the home.¹⁰⁰ After *Katz*, the Fourth Amendment’s protection became far broader, because it protected an individual’s “reasonable expectation of privacy” not only within certain well-marked zones or enclaves, but everywhere that circumstances might give rise to such an expectation.¹⁰¹

95. *Id.* at 465.

96. *Id.* at 473 (Brandeis, J., dissenting).

97. *Id.* at 478 (emphasis added).

98. 388 U.S. 41 (1967).

99. 389 U.S. 347, 353 (1967).

100. See, e.g., *Weeks v. United States*, 232 U.S. 383, 398 (1914) (finding the seizure of letters from the defendant’s home to be a direct violation of his constitutional rights under the Fourth Amendment).

101. This is how one commentator interpreted *Katz* the year after it was decided: “The Supreme Court is moving toward a redefinition of the scope of the Fourth Amendment. *Katz v. United States* . . . indicates that the Court is now prepared to release the Fourth Amendment . . . from the moorings of precedent and determine its scope by the logic of its central concepts.” Edmund W. Kitch, *Katz v. United States: The Limits of the Fourth Amendment*, 1968 SUP. CT. REV. 133, 133; see also LAWRENCE LESSIG, *CODE AND OTHER LAWS OF CYBERSPACE* 117 (1999) (describing how *Katz* attempted to reinedy the trespass theory of privacy by “linking the Fourth Amendment to a more direct protection of privacy” which protected “people, not places”).

While the above picture is not inaccurate, it portrays *Katz* and its reasonable expectations test as more revolutionary than it actually was. One reason is that in figuring out how to apply *Katz* to new fact situations, most courts have relied not on the majority opinion by Justice Stewart, but on the concurrence by Justice Harlan. Harlan's opinion did not so much abandon the doctrine of constitutionally protected areas as update it to take account of new technologies for electronic surveillance.¹⁰² More specifically, the doctrine of constitutionally protected areas was modernized by Justice Harlan (and subsequent Supreme Court cases) in two fundamental ways.

First, the Court refined its protection of "constitutionally protected areas" to guard against the kinds of technology that Brandeis was most obviously concerned about in his *Olmstead* dissent: technology that allowed the government to make intangible and surreptitious "entries" into traditional privacy zones (most notably the home itself).¹⁰³ In *United States v. Karo*, for example, the Court barred the government from using a beeper to track a defendant inside his house.¹⁰⁴ In *Kyllo v. United States*, it barred police outside from using forward-looking infrared (FLIR) technology to "see"—in heat measurements—details about the interior of a home.¹⁰⁵ As Justice Harlan noted in his *Katz* concurrence, "electronic as well as physical intrusion into a place that is . . . private may constitute a violation of the Fourth Amendment."¹⁰⁶

Second, apart from protecting the home and other places where individuals were traditionally able to exclude others, the Court recognized the importance of new "constitutionally protected areas" where technology has made it possible, desirable, and virtually unavoidable for people to convey information about their personal desires and preferences. Thus, in a world where much communication cannot take place except over public phone lines, and people make calls from public places, one could hardly expect an individual to succeed in avoiding the discussion of family affairs or personal anxieties over such phone lines. Justice Harlan emphasized this point also in his *Katz* concurrence: "an enclosed telephone booth is an area where, like a home, and unlike a field, a person has a constitutionally protected reasonable expectation of privacy."¹⁰⁷ Moreover, as David Sklansky has emphasized, in the modern world, such "constitutionally

102. David A. Sklansky, *Back to the Future: Kyllo, Katz, and Common Law*, 72 MISS. L.J. 143, 158 (2002).

103. *Id.* at 159–60.

104. 468 U.S. 705 (1984).

105. 533 U.S. 27 (2001).

106. *Katz v. United States*, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring).

107. *Id.* at 360 (Harlan, J., concurring).

protected zones” are not only physical but also virtual. Private activity and communication occurs not only in homes, offices, or enclosed phone booths, but also in Internet chat rooms, web sites, and other electronic environments.¹⁰⁸ Even if a government wiretap (or bugging device on a phone booth) intercepts conversations that take place completely outside the home (for example, between a husband and wife who are talking, respectively, from a public phone booth and a cell phone), this fact does not eliminate individuals’ privacy interests in such conversations.

Thus, just as Justice Kennedy has sought recently in the context of First Amendment “public forum” doctrine to modernize the notion of a “traditional public forum” where free speech protections have especially strong force vis-à-vis other interests of the public,¹⁰⁹ Justice Harlan tried in *Katz* to preserve but modernize the notion of specific enclaves where Fourth Amendment privacy protections have especially strong force.¹¹⁰

Indeed, Justice Harlan not only tried to modernize the doctrine of constitutionally protected zones, he succeeded—to such an extent that his concurring opinion helped undercut the majority’s attempt to give privacy protection stronger force in public life.¹¹¹ In contrast to Harlan’s updating of the doctrine of constitutionally protected zones, the Court’s majority opinion in *Katz* explored another more radical challenge to the *Olmstead* framework. It had considered the possibility that privacy protections might in a sense be

108. Video surveillance gives rise to a more difficult problem, because, unlike surveillance of chat rooms or e-mail exchanges, the activities it captures *do not* occur in an environment that is insulated against intrusions by nonparticipants in a given public activity. Even someone who is not a participant in a conversation or activity on a public street can share the same space with those who are.

109. See *Int’l Soc’y for Krishna Consciousness v. Lee*, 505 U.S. 672, 698 (1992) (Kennedy, J., concurring) (noting that “failure to recognize the possibility that new types of government property may be appropriate forums for speech will lead to a serious curtailment of our expressive activity” and that “[o]ne of the places left in our mobile society that is suitable for discourse is a metropolitan airport”); see also *Denver Area Educ. Telecomm. Consortium Inc. v. FCC*, 518 U.S. 727, 802–03 (1996) (Kennedy, J., concurring in part and dissenting in part) (“Minds are not changed in streets and parks as they once were. To an increasing degree, the more significant interchanges of ideas and shaping of public consciousness occur in mass and electronic media.”).

110. It is interesting to note that, as Morgan Cloud points out, Justice Butler, one of the dissenters in *Olmstead* other than Brandeis, proposed a similar updating of the property-based version of trespass theory in existence at the time of *Olmstead* to cover the wiretapping involved in that case. See Morgan Cloud, *Rube Goldberg Meets the Constitution: The Supreme Court, Technology and the Fourth Amendment*, 72 *MISS. L.J.* 5, 18 (2002). As Cloud notes, Butler felt that “the Court’s traditional property-based theories could have been employed to encompass technological surveillance” and he tried to “analogiz[e] private conversations to private property.” *Id.* (citing *Olmstead v. United States*, 277 U.S. 438, 485, 487–88 (1928) (Butler, J., dissenting)).

111. See Sklansky, *supra* note 102, at 158 (asserting that Harlan’s view that the Fourth Amendment’s protection is limited to locations is “hard to reconcile with the Court’s grand proclamation . . . that ‘the Fourth Amendment protects people, not places’”).

made portable and taken with people as they traveled from place to place.¹¹² Under such a conception of the Fourth Amendment, individuals might have constitutional privacy protection even where they were least able to exclude others from being present or to place limits on what is seen and heard: in parks, streets, and public squares. As one state court later put it in elaborating upon this strand of *Katz* when analyzing video surveillance: “A person has a ‘halo’ of privacy *wherever he goes* and can invoke a protectable right to privacy wherever he may legitimately be . . . be it a public park or a private place”¹¹³ As noted earlier, *Katz* itself made clear that its goal was to extend Fourth Amendment privacy rights beyond those particular zones or sites traditionally regarded as “private.”¹¹⁴ Holding that the Fourth Amendment protects people, not places, it stressed that “what [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.”¹¹⁵

Such language accords with powerful intuitions about privacy. Many Americans would probably object to the idea that they become fair targets for minute-to-minute surveillance or recording as soon as they walk out of a home or office. The problem with this aspiration in *Katz* is that it predictably leads to a blurring of the boundaries between what is private and what is public and open to view, and seems to leave both law enforcement officials and others with little guidance as to what is covered by Fourth Amendment protections. After all, to clearly communicate what it is we regard as private outside of the Fourth Amendment context, we often rely on barriers that block sight or hearing. As William Heffernan notes, “a closed door” or “a sealed envelope” provides a cue that what lies behind or inside of it is not to be observed or read.¹¹⁶ If we take away such cues, and insist that certain activities or objects are private and should be safeguarded against observation *even when they are visible*, we need to provide some substitute method of marking off these activities or objects as deserving of protection against observation.

The Court in *Katz* suggested that a person might provide signals about what “he seeks to preserve as private” by “knowingly expos[ing]” it or not doing so.¹¹⁷ But it did not clearly define how one might do so other than by

112. See *Katz*, 389 U.S. at 359 (“Wherever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures.”).

113. *State v. Bonnell*, 856 P.2d 1265, 1275 (Haw. 1993) (internal quotations and citations omitted) (emphasis added).

114. *Katz*, 389 U.S. at 350–53.

115. *Id.* at 351.

116. William C. Heffernan, *Fourth Amendment Privacy Interests*, 92 J. CRIM. L. & CRIMINOLOGY 1, 59 (2001).

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

concealing or not concealing it.¹¹⁸ It was perhaps this gap in the majority's reasoning that led Justice Harlan to translate the majority's "knowing exposure" test back into the framework of constitutionally protected zones. Justice Harlan acknowledged and endorsed the majority's insistence that the touchstone of Fourth Amendment privacy is what an individual "seeks to preserve as private."¹¹⁹ To capture this notion of individual intent, Justice Harlan built his two-part test for identifying a Fourth Amendment search around the notion of individual expectations. Government surveillance of an activity amounted to a search (1) if it intruded upon an actual (subjective) expectation of privacy and (2) if that "expectation [was] one that society is prepared to recognize as 'reasonable.'"¹²⁰ However, Justice Harlan also made clear that an individual's expectation of privacy was most likely to be reasonable if it arose in a private place. He stressed that one cannot tell what protection the Fourth Amendment offers to people without "reference to a 'place.'"¹²¹ While an individual would have a reasonable expectation of privacy in a traditionally private place, such as a home,¹²² or a "temporarily private place," such as a phone booth,¹²³ such an expectation would not be reasonable for "conversations in the open."¹²⁴

Courts and commentators have followed Harlan's lead. In *United States v. Tabor*,¹²⁵ for example, the Second Circuit noted that the requirement that society recognize an expectation as reasonable "appears to focus less on a person's actions and more on the place in which he acts."¹²⁶ Likewise, in his influential treatise on search and seizure law, Wayne LaFave takes the position that "[u]nder the *Katz* expectation of privacy test, particular attention must be given to the nature of the place at which the observed objects or activities are located, for this will bear directly upon whether there was a justified expectation of privacy as to those objects or activities."¹²⁷

118. See Melvin Gutterman, *A Formulation of the Value and Means Models of the Fourth Amendment in the Age of Technologically Enhanced Surveillance*, 39 SYRACUSE L. REV. 647, 667 (1988) (noting that "*Katz* identified the right of privacy as the basic interest to be protected by the Fourth Amendment, but neither the manner in which this protection was to be assured nor the extent of its protections were delineated").

119. See *Katz*, 389 U.S. at 361 (Harlan, J., concurring) ("[O]bjects, activities, or statements that [a man] exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited.").

120. *Id.*

121. *Id.*

122. *Id.* at 360.

123. *Id.* at 361.

124. *Id.*

125. 635 F.2d 131 (2d Cir. 1980).

126. *Id.* at 137.

127. LAFAVE, *supra* note 52, § 2.2(c), at 419.

The Supreme Court has also given its support to an interpretation of reasonable expectations tied firmly to particular places. In *United States v. Oliver*, the Court held that *Katz*'s reasonable expectation of privacy test did nothing to weaken the open fields doctrine.¹²⁸ This doctrine, adopted by the Court in 1924, provides that the protection of the Fourth Amendment "is not extended to the open fields."¹²⁹ The *Oliver* Court stressed that, "as a practical matter [open fields] usually are accessible to the public and the police in ways that a home, an office, or commercial structure would not be" and therefore an "expectation of privacy in open fields is not an expectation that 'society recognizes as reasonable.'"¹³⁰ While the Court was specifically analyzing fields rather than streets or public squares, its logic seems to apply even more forcefully to the latter areas, to which the police and the public have greater access than they do to the privately-owned fields in *Oliver*.

By salvaging the concept of constitutionally protected areas, Justice Harlan effectively postponed a more radical challenge to the *Olmstead* framework, one which could protect anonymity and other forms of privacy even in public. Ironically, it was Justice Harlan himself who later revisited this challenge and provided a starting point for addressing it that was significantly more promising than the one that the majority had sought to provide in *Katz*.¹³¹ Indeed, Justice Stewart's majority opinion may bear as much responsibility as Harlan's concurrence for the failure to extend constitutional privacy protections to public spaces. Even without the gloss imposed by Harlan's concurring opinion, Stewart's focus on "knowing exposure" might have led courts to focus on whether a person bothered to conceal his activities behind a wall or a barrier, because that is the most common signal one can give of whether these activities are private. Stewart's opinion, in any event, did not provide additional guidance as to when activities in public space should count as "private," and this silence helped assure that Harlan's narrower rule would prevail. As Edmund Kitch stressed shortly after *Katz* was decided, the Court could not successfully redefine Fourth Amendment law without "a limiting principle to replace that of *Olmstead*."¹³² Its failure to provide any such limiting principle left future courts nothing to rely upon except the familiar distinction between private and public areas.

Individuals, of course, may still claim Fourth Amendment protection against an unreasonable physical search of their person in public spaces. Courts have held, for example, that a pat-down of outer clothing by a police

128. 466 U.S. 170 (1984).

129. *United States v. Hester*, 265 U.S. 57, 59 (1924).

130. *Oliver*, 466 U.S. at 179.

131. See *infra* subpart III(B).

132. Kitch, *supra* note 101, at 134.

officer in a street or a park is a search.¹³³ Likewise, when an official searches a handbag or a suitcase, that is a search, because such containers, like walls, provide a clear and accepted means of concealing items from others' view.¹³⁴ What *Katz* did not provide was a form of constitutional privacy protection that might protect even those public activities that are visible or audible.

In short, while the *Katz* majority attempted to fashion constitutional safeguards that would protect us in streets and parks as well as in homes and offices, it could not find a way to do so. As David Sklansky observes, "[t]he decision in *Katz* seemed to promise a Fourth Amendment that was less tied to specific locations, and therefore somehow more modern. The Justices keep renewing that promise, but they have never figured out how to make good on it."¹³⁵ Fortunately, as explained below in Part III, the Supreme Court does not need to make good on this promise because there is another, more viable approach to protecting privacy and anonymity in the public sphere. Instead of persisting in trying to sever privacy from location, courts might instead begin protecting those forms of privacy that are *distinctive* to public places (along with the privacy they already protect in homes and other enclosed areas).

II. The Technological Challenge to *Katz*: Watching, Tracking, Identifying, and Detecting Private Details in Public Spaces

The lack of safeguards against monitoring in public places was generally of little consequence in the decades after *Katz*. Although the government was free to track and observe individuals in public places, the use of such tracking was limited by important practical constraints.¹³⁶ Tracking and observing an individual takes significant effort. Moreover, if an investigator is hoping to find specific information about particular people, substantial time may pass before his surveillance picks up something useful. It may be a substantial burden for him to listen to hours of recorded conversations or sift through piles of intercepted data.¹³⁷

133. See, e.g., *Terry v. Ohio*, 392 U.S. 1 (1968).

134. See *United States v. Ross*, 456 U.S. 798, 822–23 (1982) (noting that Fourth Amendment protection applies to a container that "conceals its contents from plain view").

135. Sklansky, *supra* note 102, at 160.

136. Of course, even given the difficulties of tracking, warrantless use of surveillance to track an innocent individual is not of little consequence to the person who is so targeted—for example, a political dissident who is scrutinized solely because of his speech. However, without significant tracking and recording capacities, the government was limited in how many such people it could follow. And even dissidents subject to police observation had more opportunity to escape such surveillance than they would in a world where all of their public activities were automatically recorded.

137. As the Supreme Court recently made clear in *Illinois v. Lidster*, 124 S. Ct. 885 (2004), the existence of such practical constraints on surveillance can have Fourth Amendment significance. The Court found little cause to worry that its approval of police information stops would lead to

But one of the hallmarks of new surveillance technologies is the degree to which they lower the costs, both in time and expense, of round-the-clock monitoring. Real-time human monitoring is no longer necessary, as videos and tracking devices can be supplemented with devices that automatically record a person's movements for viewing at a later time. While government monitors might have once needed impossibly large and unmanageable libraries of video footage or other records to capture significant portions of a person's life (and tremendous amounts of tedious labor to search such records) they can now store massive amounts of information in computer memory banks and then have computers rapidly search and return the information they are looking for.¹³⁸

Taking a page from Lewis Padgett's science fiction world, governments have also used such technologies to transform public space into a medium that itself records movements. Even those individuals who limit their contact with modern electronic technologies—by shunning cell phones or Internet credit card transactions, for example—might now find that they leave a record as they move through public space. Their movements might be recorded by ubiquitous camera networks or by "intelligent transportation systems" that trace the movements of automobiles on public highways. Such transformations bring to physical space many of the same worries that have recently been raised about the tracking of our movements in virtual space (through use of cookies or "web click trails").¹³⁹ As science fiction writer William Gibson recently noted of such technological transformations, "the street itself seem[s] to have evolved" into a "sensory apparatus."¹⁴⁰

Faced with these dramatic alterations in the physical scaffolding for our individual liberties and rights of privacy, the response of American courts has often been surprisingly nonchalant. Indeed, courts have sometimes acted

"unreasonable proliferation of police checkpoints" because "[p]ractical considerations—namely, limited police resources and community hostility to related traffic tie-ups—seem likely to inhibit any such proliferation." *Id.* at 890. In Part IV, I look more closely at how courts should analyze practical constraints which prevent expansion of a search (or the use of a search for purposes other than those which justify it).

138. As one commentator notes, "[t]he digitization of images caught on video allows for the easy and inexpensive reproduction and transferability of video images. It also allows the digital data representing these images to be easily stored for an indefinite period of time." Christopher S. Milligan, Note, *Facial Recognition Technology, Video Surveillance, and Privacy*, 9 S. CAL. INTERDISC. L.J. 295, 303 (1999). Facial recognition has the potential to make searches even less burdensome for investigators in need of particular information. For instance, "facial recognition software could search hundreds of hours of news video to find all occurrences of a political figure or known individual." Orlans, *supra* note 27, at 72.

139. See Jeffrey Rosen, *The Eroded Self*, N.Y. TIMES MAG., Apr. 30, 2002, at 46, 52 (noting how various technologies related to the Internet make it "a world where most electronic footsteps are recorded and all records can be instantly retrieved").

140. William Gibson, *The Road to Oceania*, N.Y. TIMES, June 25, 2003, at A25.

as though these novel and far-reaching technological developments are not really novel at all—but rather more effective and cost-efficient variants of long-accepted methods of police work. Such an analogy of the new to the old is in fact a familiar part of the modern Fourth Amendment jurisprudence and has often appeared in the Supreme Court's applications of the *Katz* test. Recording a conversation on audiotape, it reasoned in *United States v. White*, is no more constitutionally problematic than remembering it and writing it down.¹⁴¹ Photographing a public scene with a powerful zoom lens, it said in *Dow Chemical Co. v. United States*, is no more a breach of constitutional privacy rights than looking at the same scene with binoculars, or for that matter with unaided vision.¹⁴² Finally, in *United States v. Knotts*, the Court found that tracking someone with the aid of a hidden beeper is just a more efficient means of tailing him as he drives down a street.¹⁴³

Such statements may seem strange in the wake of the Court's recognition in *Katz* that Fourth Amendment jurisprudence must take adequate account of new technological developments. But they make perfect sense if one accepts the account of *Katz* presented in Part I. Under this account, technological change acquires constitutional significance not when it makes state monitoring of individuals considerably more extensive or intense but only when it somehow pierces the walls of a house, a telephone booth, or some other enclosed physical, virtual, or communicative space. Where expanding methods of surveillance leave such recognized private zones untouched, courts applying the *Katz* framework tend to declare them outside the scope of the Fourth Amendment. For example, in *Dow Chemical Co.*, the Supreme Court acknowledged that a sophisticated camera had revealed details of a company's physical plant that would otherwise have remained invisible to government agents.¹⁴⁴ But the Court insisted that the use of such magnification technology did not cross the constitutionally-significant boundary line one crosses when using "[a]n electronic device to penetrate walls or windows."¹⁴⁵

But a closer look at recent search and seizure decisions reveals the building blocks for an alternative Fourth Amendment jurisprudence. In a

141. 401 U.S. 745, 750–52 (1971). As one lower court put it: the "mere fact that the observation is . . . recorded on film rather than in a supervisor's memory, does not transmogrify a constitutionally innocent act into a constitutionally forbidden one." *Vega-Rodriguez v. P.R. Tel. Co.*, 110 F.3d 174, 181 (1st Cir. 1997).

142. 476 U.S. 227, 238 (1986) (noting that "[t]he mere fact that human vision is enhanced somewhat . . . does not give rise to constitutional problems").

143. 460 U.S. 276, 282 (1983) (involving a transmitter hidden in a drum of chemicals typically used in the manufacture of illicit drugs).

144. 476 U.S. at 238.

145. *Id.* at 239.

number of cases, courts appear to recognize that, even when official surveillance is focused only on public spaces, it can present a significant threat to core liberty and privacy interests. The most obviously relevant caselaw for purposes of this Article is the caselaw on video surveillance itself.¹⁴⁶ But emerging video surveillance systems undermine privacy not only by acquiring images, but also by magnifying details, tracking or reconstructing people's movements, and identifying people by using facial recognition software. It is therefore useful to look at how the law deals with all of these technologies of public surveillance and to understand how its treatment of such public surveillance compares to its treatment of new detection technologies—like X-ray devices or thermal imagers—that *do* “penetrate walls or windows.”¹⁴⁷

A. Video Surveillance

There is little dispute that, in some forms, video surveillance can severely undermine privacy and freedom. Individuals will have little space for private action if they constantly feel as though they are being watched by an unseen audience. When George Orwell wanted to describe a society bent on crushing individuality, he made video surveillance a central part of it: “telescreens” extended the government’s gaze into homes, workplaces, and street corners.¹⁴⁸ And at least some courts have echoed Orwell’s dystopian vision of the future when addressing Fourth Amendment challenges to video surveillance. In a 1984 decision, for example, the Seventh Circuit warned that if left unrestricted, “television surveillance . . . could be grossly abused—to eliminate personal privacy as understood in modern Western nations.”¹⁴⁹ The court did not bar video surveillance entirely. On the contrary, it found that, given the gravity of the threat it was facing, the government had acted permissibly when it gathered surreptitious video

146. *E.g.*, *United States v. Taketa*, 923 F.2d 665 (9th Cir. 1991); *United States v. Mesa-Rincon*, 911 F.2d 1433 (10th Cir. 1990); *United States v. Torres*, 751 F.2d 875 (7th Cir. 1984).

147. The classification of technologies that I use to organize this discussion bears some resemblance to that which the ABA’s Standards on Electronic Surveillance uses to distinguish different forms of “technologically-assisted physical surveillance.” *See* ABA STANDARDS OF CRIMINAL JUSTICE, ELECTRONIC SURVEILLANCE, SECTION B: TECHNOLOGICALLY-ASSISTED PHYSICAL SURVEILLANCE (3d ed. 1999), at 2. The ABA divides such surveillance into five broad categories, based on the kind of information that each surveillance technology obtains: (A) video surveillance, such as that made possible by public cameras, (B) tracking devices, such as beepers, sonar devices, and “Intelligent Vehicle Highway Systems,” (C) illumination devices, such as flashlights, (D) telescopic devices, and (E) detection devices, such as heat sensors and metal or explosives detectors. *Id.* at 2–3. I also analyze biometric and face recognition technologies, which the ABA has not classified as a separate kind of physical surveillance.

148. *See* ORWELL, *supra* note 8, at 4.

149. *Torres*, 751 F.2d at 882.

footage of terrorists' bomb-making activities.¹⁵⁰ But Judge Posner's decision subjected video surveillance within private homes or businesses to strict constitutional limits, intended to ensure that such surveillance takes place only when it is necessary.¹⁵¹ Before receiving a warrant to install cameras in homes or other private places, police must satisfy four criteria analogous to those they must meet under the Wiretap Act.¹⁵² They must (1) show that normal (less intrusive) methods have failed or are not worth trying, (2) describe particularly the nonverbal conduct to be surveilled, (3) limit the period of interception to no longer than is necessary to achieve stated objectives, and (4) minimize the interception of conduct unrelated to the objectives of the warrant.¹⁵³ Six other circuits have since imposed the identical or nearly identical constraints on video surveillance and repeated the Seventh Circuit's warning that video surveillance can be incredibly destructive of privacy and must be carefully limited.¹⁵⁴

But such vigilance against video monitoring has been reserved almost entirely for cases where police wish to tape or televise activities within a home or private office. Where defendants have complained of being videotaped in public environments, courts have almost always found the Fourth Amendment inapplicable. Thus, although the Tenth Circuit stressed that "[t]he use of a video camera is an extraordinarily intrusive method of searching"¹⁵⁵ and demanded extensive justification from government agents who had used such a surveillance method to monitor the interior of a private business,¹⁵⁶ it flatly rejected a complaint about video cameras mounted on

150. *Id.* at 885.

151. *Id.*

152. This parallel to the Wiretap Act was not a coincidence: the Seventh Circuit explicitly decided to "borrow the warrant procedure of Title III, a careful legislative attempt to solve a very similar problem, and hold that it provides the measure of the government's constitutional obligation of particular description in using television surveillance to investigate crime." *Id.* Other courts have adopted the same approach. See *United States v. Mesa-Rincon*, 911 F.2d 1433, 1438 (10th Cir. 1990) ("We simply look to Title III for guidance in implementing the fourth amendment in an area that Title III does not specifically cover."); *United States v. Koyomejian*, 970 F.2d 536, 542 (9th Cir. 1992) (quoting *Mesa-Rincon* and adopting the same approach).

153. *Torres*, 751 F.2d at 883–85. As the Seventh Circuit explained, these four requirements are analogous to the four requirements of "particularity" in the Wiretap Act, 18 U.S.C.A. §§ 2510–2520 (West 2000 & Supp. 2003), designed as "safeguard(s) against electronic surveillance that picks up more information than is strictly necessary" in violation of "the Fourth Amendment's requirement of particular description." *Id.* at 883–84.

154. *United States v. Williams*, 124 F.3d 411, 416 (3d Cir. 1997); *United States v. Falls*, 34 F.3d 674, 680 (8th Cir. 1994); *Koyomejian*, 970 F.2d at 542; *Mesa-Rincon*, 911 F.2d at 1438; *United States v. Cuevas-Sanchez*, 821 F.2d 248, 252 (5th Cir. 1987); *United States v. Biasucci*, 786 F.2d 504, 510 (2d Cir. 1986).

155. *Mesa-Rincon*, 911 F.2d at 1442.

156. *Id.* at 1437–38.

telephone poles on a street outside of the defendant's residence.¹⁵⁷ In contrast to cameras hidden in a home or office, these cameras captured nothing more than "what any passerby would easily have been able to observe."¹⁵⁸ In short, the crucial factor for the Tenth Circuit was whether the surveillance took place "inside" or "outside."¹⁵⁹ Indeed, this dichotomy was so important that the Court of Appeals refused to deviate from it even though the inside surveillance (analyzed in the Tenth Circuit's *Mesa-Rincon* decision) took place in a business where there was only "a 'medium' expectation of privacy,"¹⁶⁰ while the outside surveillance (analyzed in the Tenth Circuit's *Jackson* case) was aimed at the area just outside someone's home.¹⁶¹

A similar stance on the constitutionality of public video surveillance has been adopted by virtually every state and federal court to address the issue.¹⁶² With this caselaw as a background, it is not surprising that even ACLU spokesmen who vigorously endorse legislative limits on unrestricted video surveillance systems have sometimes conceded that "it is not unconstitutional to place cameras in public places."¹⁶³

But a closer look at the caselaw reveals greater nuance in judicial analysis of public video surveillance. First, a number of courts which have objected to video surveillance in enclosed and arguably "private" environments have set forth analyses which appear to raise constitutional

157. *United States v. Jackson*, 213 F.3d 1269, 1281 (10th Cir. 2000).

158. *Id.*

159. *Id.*

160. *Mesa-Rincon*, 911 F.2d at 1443.

161. *Jackson*, 213 F.3d at 1276.

162. See, e.g., *United States v. Sherman*, 990 F.2d 1265 (table), 1993 WL 77236, at *2 (9th Cir. Mar. 18, 1993) (finding no expectation of privacy on a mountaintop because it was visible to the naked eye); *State v. Augafa*, 992 P.2d 723, 724 (Haw. Ct. App. 1999) (holding no expectation of privacy under article I, section 7 of the Hawaii Constitution against video surveillance of the front of a bar that was otherwise observable with the naked eye); *State v. Holden*, 964 P.2d 318, 321 (Utah Ct. App. 1998) (finding no expectation of privacy against being videotaped in a front yard where police "merely recorded on tape what was open to public view") (internal quotation and citation omitted); *State v. Fellows*, No. 34141-3-1, 1997 WL 43666, at *3 (Wash. Ct. App. Feb. 3, 1997) (finding no expectation of privacy against videotaping the front of a residence otherwise visible to the naked eye); *State v. Clemmons*, No. 5233-7-1, 1996 WL 146721, at *2 (Wash. Ct. App. Apr. 1, 1996) (finding no expectation of privacy against a videotape of actions on a public street); *People v. Lynch*, 179 Mich. App. 63, 69-70 (1989) (finding no expectation of privacy in the common area of a public restroom); *Sponick v. City of Detroit Police Dep't*, 49 Mich. Ct. App. 162, 198 (1973) (finding no expectation of privacy in a public tavern for videotaped images that "any member of the general public would see if he entered the tavern as a patron").

163. See *Richmond to Employ Surveillance Cameras*, *supra* note 19 (quoting an ACLU representative); see also *Heinzmann*, *supra* note 18 (noting that "[a] spokesman for the American Civil Liberties Union said the cameras, if used only in public areas as promised, do not present constitutional problems").

doubts about public video surveillance as well.¹⁶⁴ The key theme in these cases is that close and sustained scrutiny can constitute a Fourth Amendment search even when casual or incidental observation from passers-by would not be. In *State v. Thomas*, for example, an Indiana state court found that the government engaged in a search when it surreptitiously videotaped a store clerk's activities behind a cash register even though these activities often occurred in plain view of store customers.¹⁶⁵ "Incidental or occasional looks by members of the public," explained the court, should not automatically leave a person vulnerable to "prolonged observation by the government from a non-public vantage point" (in this case, from a video camera recording through a hole in the ceiling).¹⁶⁶

Other courts have reached a similar conclusion. In *United States v. Taketa*, for example, the Ninth Circuit agreed with the government that the defendant had "no general privacy interest" in his colleague's office, but found that "he may have an expectation of privacy against being videotaped in it."¹⁶⁷ The video surveillance at issue, said the court, was unlike a physical search of the individual's possessions because it was "directed straight at him, rather than being a search of property he did not own or control," because he was present for the video search, and because the "silent, unblinking lens of the camera was intrusive in a way that no temporary search of the office could have been."¹⁶⁸ In *State v. Bonnell*, the Hawaii Supreme Court found on similar grounds that "[w]hatever the general privacy interest the defendants may or may not have had in the [employee] break room," they did have a constitutional right against being subjected to television surveillance there.¹⁶⁹ None of these courts was willing to state that individuals' right against being videotaped extended to parks and streets as well as office space.¹⁷⁰ Indeed, the Ninth Circuit recently found that while, under *Taketa*'s holding, "[a] person has a stronger claim to a reasonable expectation of privacy from video surveillance than against a manual

164. See, e.g., *United States v. Taketa*, 923 F.2d 665, 677 (9th Cir. 1991) (hypothesizing that even where no general privacy right exists, a person may have an expectation of privacy against being videotaped in a public area); *State v. Thomas*, 642 N.E.2d 240, 246 (Ind. Ct. App. 1994) (indicating that certain public surveillance may violate the Fourth Amendment).

165. 642 N.E.2d at 245-46.

166. *Id.* at 246.

167. 923 F.2d at 676.

168. *Id.* at 677.

169. 856 P.2d 1265, 1277 (Haw. 1993).

170. *Bonnell*, while applying its holding to a workplace area and stressing that the cameras were aimed at an inside space, *id.* at 1276, suggested that a reasonable expectation of privacy can also be violated in parks and other open areas because people have privacy in their *person*, not because public places can be in any sense private, *id.* at 1275. It did not, however, explain when and how video surveillance might violate such a personal right to privacy in an open area.

search,” such protection does not extend to “activities already visible to the public.”¹⁷¹ But while cases such as *Taketa* have resisted extending Fourth Amendment protections to public places, their logic seems to lead in that direction: if the unrelenting gaze of a video camera can corrode an individual’s privacy even in places where he has no general privacy interest, it is not clear why such a gaze is any less harmful when it tracks him from block to block than it is when it comes from a fixed camera at a store or workplace. In either environment, someone who knows he is being closely and steadily watched (or knows that he may be subject to such scrutiny) is likely to feel the significant discomfort and loss of freedom that comes from being under an official magnifying glass.

Other cases provide yet another reason to doubt that public video surveillance will remain forever shielded from Fourth Amendment scrutiny.¹⁷² While federal and state court cases have been almost unanimous in permitting the government to aim cameras at *specific* individuals or areas within public places, none of these courts has carefully considered the constitutional implications of mass video surveillance in a town or city. The few courts that have touched on such mass surveillance have hinted that it might well be subject to Fourth Amendment limits. The Vermont Supreme Court, for example, did this even as it rejected a defendant’s claim that the government had violated the Fourth Amendment when it taped him attending to his marijuana garden in “unposted, open land.”¹⁷³ Having denied the defendant Fourth Amendment protection, it hastily added that matters might be different “where video surveillance is *aimed indiscriminately at public places* and captures lawful activities of many citizens in the hope that it will deter crime or capture what crime might occur.”¹⁷⁴ In other words, public video surveillance will not automatically escape constitutional scrutiny simply because it occurs in public. Whether it triggers the Fourth Amendment will also depend on the scale of the surveillance and the degree to which it is constrained by the need for suspicion of criminal wrongdoing.

The Supreme Court of Alaska recently followed the Vermont Supreme Court in stressing the latter of these two factors. It held that the Fourth Amendment did not shield an employee’s actions in plain view of customers from video monitoring,¹⁷⁵ but went on to note that such monitoring might well have triggered constitutional protections if it “had not been initiated for a legitimate purpose—the detection of theft—and had not been based on

171. *United States v. Gonzalez*, 328 F.3d 543, 548 (9th Cir. 2003).

172. *E.g.*, *State v. Costin*, 720 A.2d 866 (Vt. 1998); *Cowles v. State*, 23 P.3d 1168, 1171 (Alaska 2001).

173. *Costin*, 720 A.2d at 869.

174. *Id.* at 870 (emphasis added).

175. *Cowles*, 23 P.3d at 1171.

reasonable grounds to believe that [the employee] was stealing.”¹⁷⁶ In other words, while warrantless videotaping in public is acceptable, *suspicionless* videotaping apparently is not.

Such a stance is somewhat odd because under existing Fourth Amendment jurisprudence, police are free to observe a person or activity without “reasonable suspicion” of criminal activity, as long as such observation does not amount to a search or seizure.¹⁷⁷ It is, after all, only searches and seizures which must be reasonable under the Fourth Amendment.¹⁷⁸ By requiring reasonableness even for a *nonsearch*, courts like those in *Cowles* and *Costin* seem to implicitly acknowledge that courts should be on guard against public video surveillance even if they do not impose constitutional constraints on the simplest forms of it.

Such cases also reveal judicial reluctance to equate new and sophisticated mass surveillance systems with the familiar, decades-old practice of pointing a camera at someone. And this reluctance is well-founded. Admittedly, the presence of cameras in public is not new: government-operated networks of public cameras first appeared decades ago. Early video systems were installed in a number of towns in New York and New Jersey, and a network of cameras funded by the New York Times and several local businesses was installed in Times Square in 1973.¹⁷⁹ Miami also experimented with video surveillance in the early 1980s.¹⁸⁰ But these systems are very different from what is emerging now. The images they captured were often too grainy or blurry to be of any help to police or to be a significant threat to individual privacy. In contrast, the new camera systems are entirely different in scale and scope. The technological advances I have already discussed—miniaturization, digitization, and scientific leaps in computer storage and processing technology—allow authorities to capture and retain substantially more detailed information about activities in public space. As the General Accounting Office has recently noted, some systems allow camera operators to “move” from city block to city block with a joystick and zoom in on activities they wish to scrutinize.¹⁸¹ Recently, the Defense Advanced Research Projects Agency (DARPA) has encouraged development of video technology that can automatically record the

176. *Id.* at 1175.

177. See *Texas v. Brown*, 460 U.S. 730, 738–39 n.4 (1983) (noting that “an officer’s mere observation of an item left in plain view . . . generally involves no Fourth Amendment search”).

178. I argue below in Part V that one possible cause of such confusion is that the “reasonable expectation” test for what constitutes a search predictably leads judges to confuse the questions of whether a search is a “search” and whether it is “reasonable.”

179. Quentin Burrows, *Scowl Because You’re on Candid Camera: Privacy and Video Surveillance*, 31 VAL. U. L. REV. 1079, 1103 (1997).

180. *Id.*

181. GEN. ACCOUNTING OFFICE, *supra* note 23, at 6.

movements of thousands of vehicles and search for and identify these “vehicles by size, color, shape, and license tag, or drivers and passengers by face.”¹⁸² According to DARPA, such technology is meant to recreate and understand wartime encounters (as signified by its name: “3-D Combat Zones”), but privacy advocates worry that it can easily be used for domestic surveillance.¹⁸³ Whatever one thinks of these impressive technological advances in video surveillance, they are not accurately described as a mere automated equivalent of human vision that captures nothing more than “what any passerby would easily have been able to observe.”¹⁸⁴ Rather, they change public space into something it would not otherwise be, something which in a sense preserves and processes records of people’s movements and activities in a way that primitive cameras (and even primitive networks of cameras) have not done before.

B. Enhancements to Video Surveillance: Tracking, Magnification, and Biometrics

It is not only the expansion of video surveillance itself that poses a challenge to the viability of the *Katz* test but also the dramatic changes occurring in technologies that supplement and enhance such surveillance. Networks of video cameras function not only as video cameras, but also, when linked together and given the capacity to identify and lock onto a person, as tracking devices. Supplemented with zoom capacities and infrared detectors, they might reveal features of a person that are normally invisible even to bystanders only a few yards away. And with the aid of biometric identification devices, they might also provide investigators with information of a sort that is not normally sensed at all. They might reveal the name of an unknown individual in a photograph or videotape, and investigators might then link this identifying information to other personal information. While such biometric devices are typically used to authenticate or identify unknown people, they can also be used to reconstruct the movements of a known person by searching a large database of footage from public streets and recognizing all places and events where a specific person has appeared on camera in a given day or week.¹⁸⁵

182. Michael J. Sniffen, *Pentagon Wants City-Wide Vision*, AKRON BEACON J., July 2, 2003, at A6.

183. See Cynthia L. Webb, *DARPA in the News . . . Again*, WASHINGTONPOST.COM (July 2, 2003), at <http://www.washingtonpost.com/wp-dyn/technology/govtit/review>.

184. As noted above, see *supra* note 157, this language comes from the Tenth Circuit’s decision in *United States v. Jackson*, 213 F.3d 1269, 1281 (10th Cir. 2000).

185. John D. Woodward, Jr., *Case Study: Super Bowl Surveillance*, in WOODWARD ET AL., *supra* note 27, at 247, 251. In other words, biometric identification devices can function as tracking devices. Tracking technology, such as that in intelligent transportation technologies, can likewise

Might such potentially invasive technologies trigger Fourth Amendment protections even if unadorned video cameras do not? There are certainly strong intuitive reasons to think that they would. Government observers can learn much more about an individual if, thanks to tracking technology, they have not merely a video snapshot of him, but an ongoing broadcast that shows the places he goes and the associates he meets.¹⁸⁶ Biometric databases allow observers to undermine the anonymity of those they watch. Powerful magnification also allows them to discern small details that a person never intended to make known to the world. If the Fourth Amendment is meant, as the Supreme Court has stated, to prevent government from entering on its own whim into “the privacies of life,”¹⁸⁷ then the modern tracking, identification, and magnification technologies would seem to be a matter of constitutional concern.

But, as with video surveillance itself, courts and many commentators have been reluctant to place any Fourth Amendment limits on such technologies except to protect the traditionally private environments of the home or office. And, as with video surveillance, this stance against extending Fourth Amendment protections into the public sphere begins to weaken when judges are confronted with versions of these technologies that do not temporarily undercut privacy or anonymity, but threaten to banish them entirely from public life.

1. *Tracking.*—In analyzing tracking technology, the Supreme Court might appear (on an initial reading) to have adopted the *Katz* approach without alteration. First, if a person “knowingly exposes” his movements to others in a public space, he has no grounds for a constitutional complaint when those others (including police) decide to take note of these movements.¹⁸⁸ Thus, the Court found no fault with the police when they planted a beeper in a container, arranged for the container to be sold to specific individuals, and then tracked the beeper, and these individuals, as they drove back to their cabin.¹⁸⁹ To be sure, police may have had good reason to be suspicious, because the container sought and acquired by the defendants

function as identification technology—it might allow observers not only to monitor the movements of a particular car or cell phone, but also to identify its owner.

186. Such tracking technology would not be unlike the powerful magic that aids Harry Potter when he uses the “Marauder’s Map” to detect and escape trouble. See J.K. ROWLING, *HARRY POTTER AND THE PRISONER OF AZKABAN* 192–93 (1999). As Rowling explains, the “truly remarkable thing” about this map was not that it showed every detail of the wizardry school where Harry learned his magical skills, but that “there were tiny ink dots moving around it, each labeled with a name in miniscule writing.” *Id.* at 193. One reveals the headmaster “pacing his study,” and another shows an instructor “bouncing around the trophy room.” *Id.*

187. *Boyd v. United States*, 116 U.S. 616, 630 (1886).

188. *Katz v. United States*, 389 U.S. 347, 351 (1967).

189. *United States v. Knotts*, 460 U.S. 276, 278 (1983).

was filled with a “precursor chemical” used in manufacturing illicit drugs. The police had received a tip that the defendants had stolen this chemical before and were recently purchasing additional containers of it.¹⁹⁰ But for the Court, such suspicious information was in this case constitutionally irrelevant. “A person traveling in an automobile on public thoroughfares,” said the Court, “has no reasonable expectation of privacy in his movements”¹⁹¹ and can raise no Fourth Amendment objection when police electronically follow or retrace those movements even without a good basis for doing so.¹⁹²

Apart from the argument that what is in public cannot be private, the Court also had a second, now-familiar Fourth Amendment argument for refusing to hold new technologies for tracking movements through public space unconstitutional.¹⁹³ To do so, it implied, would confine law enforcement to primitive means for detecting and investigating evidence of crime.¹⁹⁴ The police did not need a warrant simply to tail a driver on a public road; therefore, the Court decided that they should not need a warrant to follow the same person on the same roads with the aid of a tracking device capable of monitoring his movements more accurately and efficiently.¹⁹⁵ As the Court put it: “[n]othing in the Fourth Amendment prohibited the police from augmenting [their] sensory faculties . . . with such enhancement as science and technology afforded them in this case.”¹⁹⁶

As the Court hastened to add in *Knotts* and made even clearer a year later in *United States v. Karo*,¹⁹⁷ these decisions did not mean that police could use the same technological enhancement to electronically follow and monitor people within homes or other private enclaves.¹⁹⁸ To search such environments, after all, police would need a warrant, and their ability to

190. *Id.*

191. *Id.* at 281. One might conceivably distinguish tracking automobiles from tracking people (for example, as they walk on sidewalks). But it is not clear why this distinction would have any basis in the Court’s existing jurisprudence. If anything, people might expect to have less expectation of privacy on the sidewalk, where their faces are visible, than they do in a car, where an observer often cannot identify a driver without information of a sort that is normally unknown even to friends or acquaintances, such as a specific license plate number.

192. *Id.* at 282.

193. *Id.*

194. *Id.*

195. *Id.*

196. *Id.*

197. 468 U.S. 705, 715 (1984). As the Court noted, “the beeper was monitored for a significant period after” it was brought into the house, and this case was thus “not like *Knotts*, for there the beeper told the authorities nothing about the interior of *Knotts*’ cabin.” *Id.*

198. See *Knotts*, 460 U.S. at 282 (noting that *Knotts* maintained “the traditional expectation of privacy within a dwelling” while in his cabin).

“enter” electronically did not relieve them of this burden.¹⁹⁹ This, of course, is simply an application of the general principle voiced in Justice Harlan’s *Katz* concurrence that “electronic as well as physical intrusion into a place that is . . . private may constitute a violation of the Fourth Amendment,” but people cannot expect the same Fourth Amendment protection—whether from familiar or new forms of observation—when “in the open.”²⁰⁰

This straightforward application of the *Katz* test came with a caveat, similar to the one which lower courts have offered for public video surveillance. Just as some of those courts have indicated that their endorsement of public video surveillance should not be read as permitting *mass suspicionless* surveillance,²⁰¹ the Court in *Knotts* stressed that universal, round-the-clock tracking of *many* citizens might well require a different constitutional analysis.²⁰² Responding to the petitioner’s claim that Fourth Amendment protection against beeper tracking was needed to prevent omnipresent monitoring of people’s movements, the Court stressed that “if such dragnet-type law enforcement practices . . . should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable.”²⁰³

At that time, the Court was able to treat such a warning as nothing more than speculation about an unlikely future.²⁰⁴ It noted that “reality hardly suggests” that this kind of dragnet searching was taking place.²⁰⁵ As Christopher Slobogin points out, it would be harder for the Court to offer the same response now.²⁰⁶ Within a matter of years, police may no longer have to go to the trouble of surreptitiously installing a beeper on each person they wish to follow because people increasingly carry or use tracking devices voluntarily in their everyday lives. For example, more companies are installing location-determining technology in the cell phones they create, and the FCC has recently ordered all companies manufacturing cell phones to do so, to ensure that 911 callers can obtain emergency assistance as quickly as possible.²⁰⁷

199. *E.g., Karo*, 468 U.S. at 715.

200. *Katz v. United States*, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring).

201. *E.g., State v. Costin*, 720 A.2d 866, 870 (Vt. 1998); *Cowles v. State*, 23 P.3d 1168, 1175 (Alaska 2001).

202. *See Knotts*, 460 U.S. at 283–84 (noting that unscrupulous use of twenty-four hour surveillance might implicate different constitutional principles).

203. *Id.* at 284.

204. *Id.*

205. *Id.* at 283.

206. Slobogin, *supra* note 38, at 215–16.

207. *See* 47 C.F.R. §§ 20.3, 20.18 (requiring mobile radio service providers to identify calling parties for 911 systems); *see also, e.g.,* Fourth Memorandum Opinion and Order, In the Matter of Revision of the Commission’s Rules To Ensure Compatibility with Enhanced 911 Emergency

More and more people likewise allow themselves to be tracked automatically when they drive their cars on public highways. Electronic tollway systems, such as E-ZPass in the Northeast,²⁰⁸ I-Pass in Illinois,²⁰⁹ and FasTrak in California,²¹⁰ register the presence of each driver who has installed a tag or transponder in her windshield, so there is no need for the driver to stop and pay.²¹¹ Such electronically-facilitated transactions make driving less burdensome, but at the cost of making it less anonymous. This trade-off characterizes numerous other features of evolving “intelligent transportation systems.” The same technologies that allow lost drivers to find out where they are, what services are nearby, and how to get where they are going²¹² also potentially allow unseen government observers to learn or record this information. Devices on roadways that collect invaluable information on traffic, weather, and road conditions can also, in many cases, collect information about the movements and driving habits of particular drivers.²¹³ This has caused worry about whether such technology will make deeper inroads into drivers’ privacy,²¹⁴ especially because the data collected by electronic tollway systems for drivers’ convenience has been subpoenaed by private lawyers in divorce cases, state agencies investigating theft and judicial misconduct, and federal agencies, including the FBI.²¹⁵

Calling Systems, 14 F.C.C.R. 10954, ¶¶ 1–4 (2000) (denying T-Mobile’s request to modify the FCC’s requirements for identifying callers for 911 systems).

208. Welcome to E-ZPass (describing the use of E-ZPass in New York and giving links to agencies that use E-ZPass in Delaware, Maryland, New Hampshire, New Jersey, Pennsylvania, and West Virginia), at <http://www.mta.nyc.ny.us/bandt/ezintro.htm> (last visited Mar. 17, 2004).

209. ISTHA I-Pass, at <http://www.illinoistollway.com/ipass/default.asp> (last visited Jan. 13, 2004).

210. FasTrak Electronic Toll Collection, at <http://www.dot.ca.gov/fastrak> (last visited Jan. 13, 2004).

211. See Joseph Turner, *Bridge Finally Gets Green Light*, NEWS TRIB. (Tacoma), Sept. 26, 2002, at B01; see also How E-ZPass Works, at <http://www.howstuffworks.com/e-zpass.htm> (last visited Jan. 13, 2004).

212. See *Intelligent Transportation Systems Help Local Governments*, NATION’S CITIES WKLY., Nov. 27, 2000, at 6 (noting that, in rural areas, “[t]ravelers can easily get lost” and “[w]hen a crash occurs, there might not be anyone around to report it”); see also Tom Kirchofer, *Cell Phone Call Becomes Collar; Researchers Need Location; Others May Get to Use It*, BOSTON HERALD, Dec. 11, 2000, at 26 (describing possible uses of cell phone location systems that “have privacy advocates worried”).

213. See Lawrence Yermack, *Intelligent Transportation System*, CONG. TESTIMONY FED. DOCUMENT CLEARING HOUSE, Sept. 10, 2001 (noting that with the “exchange of information between equipped vehicles and the infrastructure . . . [v]ehicles will report on the rate at which traffic is flowing, the condition of the roads, weather conditions, etc.”), available at 2001 WL 26186308; see also Bob Jennings, *Invisible Passengers*, SUN-HERALD (Sydney), Oct. 15, 2000, at 4 (asserting that ITS systems can “automatically summon[] emergency services in the event of a crash and provide[] the driver with early warnings about traffic snarls”), available at 2000 WL 23721196.

214. See, e.g., Jennings, *supra* note 213 (quoting Phil Agre’s statement that “[w]e could end up with an utterly pervasive monitoring of travellers’ movements”).

215. *I-Pass Takes a Toll on Crime*, MILWAUKEE J. SENTINEL, Oct. 13, 2002, at 24A.

Radio transmitting devices may also allow officials and others to trace the paths not only of our phones and automobiles, but of numerous other products we cannot do without. For instance, various companies have been considering the use of radio frequency identification (RFID) tags to track the merchandise people buy.²¹⁶ Fearful of kidnapping, some people have considered installing trackable computer chips into their own bodies (or those of their children).²¹⁷ And with networked cameras appearing over numerous cities, authorities can more easily track people as they walk down a street, even if they are not equipped with a device that emits or receives radio signals.

One might argue that the spread of these new tracking technologies gives courts reason to leave them unbounded by any constitutional constraints: if people have voluntarily decided to use cell phones and electronic tollways, and thus, to trade the privacy of their movements for safety and convenience, why should the Fourth Amendment stand in their way? But such an argument does not dispel the concerns that led the Court to qualify its holding in *Knotts*.²¹⁸ That people voluntarily submit to some forms of tracking technology—like that pinpointing the location of 911 callers—does not mean that they should be left with no constitutional safeguards against other forms of tracking imposed upon them without their individual consent, such as inescapable tracking by cameras. Nor should such consent be understood to allow government to take any more privacy in return for safety or traffic benefits than is necessary. People might willingly allow themselves to be located when they make a 911 call or require roadside assistance, but also reasonably expect that government officials will need a warrant to track their calls or their cars for any other purpose.

216. See, e.g., Kevin Marron, 'Silent Commerce' Starts to Make Noise, *GLOBE & MAIL* (Toronto), Sept. 27, 2002, at B13 (describing the push to include a wireless computer chip in "[e]very carton of milk, every package of pills and every one of the other quadrillions of items manufactured each year"); see also Rachel Ross, *Radio Frequency Tags Gain Ground*, *TORONTO STAR*, Mar. 17, 2003, at D03 (hailing the potential usefulness of wireless computer chips but cautioning that, to protect consumers' privacy, limits must be imposed on the information the chips may track).

217. See, e.g., Julie Scheerers, *A Satellite Baby-Sitting Service*, *WIRED NEWS* (May 2, 2002), at <http://www.wired.com/news/technology/0,1282,52253,00.html>; Julia Scheeres, *Kidnapped? GPS to the Rescue*, *WIRED NEWS* (Jan. 25, 2002), at <http://www.wired.com/news/business/0,1367,50004,00.html>; Maureen Fan, *Location Tracking: An Opportunity and a Battlefield*, *STAMFORD ADVOC.*, Nov. 18, 2002, at 1; see also Christopher Newton, *Foes Fear Device Could Chip at Privacy*, *ST. LOUIS POST-DISPATCH*, Mar. 3, 2002, at E8 (describing a privacy advocate's concern over "function creep," in which a device is slowly "used for more than it was intended").

218. See *United States v. Knotts*, 460 U.S. 276, 285 (1983) (distinguishing permissible police activity from similar activity used to monitor people within homes or private enclaves).

2. *Magnification*.—The Supreme Court's response to use of magnification with visual surveillance has been very similar. In fact, when the EPA used powerful map-making cameras to take detailed pictures of a chemical plant (magnified by a factor of 240) from an airplane, the Court's response was built around the same two points that formed the core of its *Knotts* decision on tracking.²¹⁹ First, said the Court, the government had pointed its camera only toward a public space where police, and others, had a perfect right to cast their eyes. The grounds of the chemical plant were "comparable to an open field" and "as such [were] open to the view and observation of persons" flying overhead.²²⁰

Second, technologically expanding or fine-tuning such observation of public space does not become constitutionally impermissible simply because it reveals details invisible to the naked eye. "The mere fact that human vision is enhanced somewhat," said the Court, "does not give rise to constitutional problems."²²¹ While federal courts have not hesitated to hold that use of a telescope to spy upon activities in the home might constitute a search,²²² the Court stressed this was not the case here.²²³

As in *Knotts*, however, the Court in *Dow Chemical* qualified this stance in dicta by hinting that some types of magnification devices might raise constitutional problems. The EPA's use of a high-power camera was acceptable, said the Court, in part because the camera had revealed only the equipment and physical layout of the plant it was photographing, and did not capture intimate details such as "a class ring" or "identifiable human

219. See *Dow Chem. Co. v. United States*, 476 U.S. 227, 238–39 (1986) (distinguishing surveillance in public areas from surveillance in private areas and upholding the use of scientific enhancements of such surveillance); cf. *Knotts*, 460 U.S. at 285 (same).

220. *Dow Chem.*, 476 U.S. at 239.

221. *Id.* at 238. Other courts analyzing magnification in a public setting have generally applied the same principle in a straightforward way, giving the government significant room to use magnification technology in public space. See, e.g., *State v. Abislaiman*, 437 So. 2d 181, 183 (Fla. Dist. Ct. App. 1983) (finding that an individual did not have a reasonable expectation of privacy when police used the zoom capacities of a surveillance camera in a hospital parking lot to peer through a car window); *State v. Bennett*, 666 P.2d 747, 750 (Mont. 1983) (finding no search when police used a telescope to observe marijuana in a subject's open backyard).

222. *United States v. Kim*, 415 F. Supp. 1252, 1256 (D. Haw. 1976) ("It is inconceivable that the government can intrude so far into an individual's home that it can detect the material he is reading and still not be considered to have engaged in a search."); *United States v. Taborda*, 635 F.2d 131, 138–39 (2d Cir. 1980) ("The vice of telescopic viewing into the interior of a home is that it risks observation not only of what the householder should realize might be seen by unenhanced viewing, but also of intimate details of a person's private life, which he legitimately expects will not be observed either by naked eye or enhanced vision.").

223. *Dow Chem.*, 476 U.S. at 237–39. The Court squarely rejected Dow Chemical's argument that the outside of a commercial plant was analogous to the "curtilage" around a home to which courts have often extended Fourth Amendment protection. *Id.* at 239.

faces.”²²⁴ Unlike the powerful cameras approved of in *Dow Chemical*, which were pointed only at a plant, the zoom lenses on cameras watching over streets and parks can be used—and likely would be used—to magnify faces, coat pockets, and other aspects of an individual’s person without a warrant.²²⁵

It is not clear that the zoom capacities of emerging video surveillance would be free of Fourth Amendment limitations, even under the Court’s current search and seizure jurisprudence.

3. *Biometrics and Face Recognition.*—“Facial recognition” technology is designed to help camera operators quickly match an unfamiliar face on a screen with an already identified face in a database, and then perhaps to a name, social security number, and other personal information in other databases.²²⁶ While it has recently been touted as a way to identify and apprehend terrorists, it is not clear how effective it is. In the recent past, such identification has been thwarted by facial hair, aging, changes in lighting, and variations in the angle between someone’s face and the camera,²²⁷ and critics point to recent tests showing poor performance in surveillance at airports and other environments.²²⁸ That facial recognition software is still imperfect is clear from DARPA’s “Face Recognition Vendor Test,” which measures how existing facial recognition systems perform under a number of different conditions.²²⁹ The most recent run of this test in 2002 showed that even the most effective current systems had difficulty identifying faces outdoors (the best recognition rate was only 50%) and that their reliability also decreased markedly when the database of faces grew beyond a relatively

224. *Id.* at 238–39.

225. *See, e.g.*, Townsend & Harris, *supra* note 11 (noting that, in London’s “ring of steel,” cameras “will be able to zoom in on the faces of drivers”).

226. SAMIR NANAVALI ET AL., BIOMETRICS: IDENTITY VERIFICATION IN A NETWORKED WORLD 65–66 (2002).

227. *See id.* at 74 (noting that “[f]actors such as direct and ambient lighting, camera position and quality, angle of acquisition, and background composition can dramatically reduce accuracy” and that “changes in user appearance seem to have an impact on many systems’ ability to identify users”); Richard E. Smith, *How Authentication Technologies Work*, in WOODWARD ET AL., *supra* note 27, at 3, 9 (noting that according to James Wayman, a scientist and expert on facial recognition systems, “unless the photograph is captured under very controlled conditions, ideally with each subject looking directly into the camera and filling the area of the photo completely, the system may have difficulty identifying the individual or even detecting his face in the photograph”).

228. *See, e.g.*, Julia Scheeres, *Airport Face Scanner Failed*, WIRED NEWS (May 16, 2002), at <http://www.wired.com/news/privacy/0,1848,52563,00.html> (noting preliminary test results indicating that the system “failed to correctly identify airport employees 53% of the time”); *see also* NIETO ET AL., *supra* note 20, at 6 (describing a recent study by the National Institute of Standards and Technology which found that digitized photos of the same person taken 18 months apart could not be matched by computers 43% of the time).

229. Face Recognition Vendor Test, at <http://www.frvt.org/default.htm> (last visited Jan. 12, 2003).

small number (when the number of the faces in the database was increased from 25 to 3,000, the identification and detection rate dropped from 77% to 56%).²³⁰

This imperfection has not stopped law enforcement from continuing to experiment with—and hold out hope for the potential of—facial recognition. Much to the outrage of privacy advocates, the Tampa police used this technology to scan the faces of those attending the 2001 Super Bowl in Tampa Bay, comparing each face with those in a police database.²³¹ Tampa subsequently installed face recognition-equipped cameras in its Ybor City entertainment district, comparing each face it captured to a database of “30,000 photographs of wanted felons and lost children.”²³² Although the city recently ended the experiment after finding the technology did not help lead police to criminals,²³³ other municipalities and agencies continue to be interested in facial recognition. Virginia Beach, Virginia has installed and continues to operate a facial recognition system that compares sunbathers and others wandering its beachfront to images of people with outstanding warrants, missing persons, and runaways.²³⁴ Other states are using facial recognition systems to guard against fraudulent acquisition of drivers licenses.²³⁵ And the flaws of existing facial recognition technologies may well be overcome by future versions of this technology being developed by private vendors and in DARPA’s “Human Identification at a Distance” program.²³⁶

230. Phillips et al., *supra* note 27, at 2, 9; see also Andrew W. Senior & Ruud M. Bolle, *Face Recognition and Its Application*, in BIOMETRIC SOLUTIONS FOR AUTHENTICATION IN AN E-WORLD, at 83, 85 (David Zhang ed., 2002) (noting that face recognition currently has “relatively low accuracy (compared to the proven performance of fingerprint and iris recognition)”).

231. Smith, *supra* note 227, at 8.

232. Jessica Reaves, *Tampa Gets Ready for Its Close-Up*, TIME ONLINE EDITION, (July 16, 2001), at <http://www.time.com/time/nation/article/0,8599,167846,00.html>; see also *Tampa Uses Cameras to Scan for Wanted Faces*, CNN.COM (July 2, 2001), at <http://www.cnn.com/2001/TECH/ptech/07/02/high.tech.security.ap>.

233. See *Fla. Police Scrap Surveillance System*, ABCNEWS.COM (Aug. 20, 2003), at http://abcnews.go.com/wire/US/ap20030820_2029.html.

234. David McGuire, *Virginia Beach Installs Face Recognition Cameras*, WASHINGTONPOST.COM (July 3, 2002), at <http://www.washingtonpost.com/ac2/wp-dyn/A19946-2002Jul3>.

235. See, e.g., Tom McGhee, *State Driver’s Licenses to be Harder to Exploit, Retail Industries Cheer Anti-Fraud Bill*, DENV. POST, May 10, 2001, at C-01 (discussing legislation enabling Colorado’s Department of Motor Vehicles to use facial recognition technology to prevent driver’s license fraud). This technology has been used in the private sector by casinos wishing to deny entry to card counters and others who have violated the casinos’ rules. *Smile! You’re on Casino Camera*, CBSNEWS.COM (Feb. 26, 2001), at <http://www.cbsnews.com/stories/2001/02126/tech/main274604.shtml>.

236. A Compendium of DARPA Programs (April 2002) (describing the HumanID program as one that will “develop methods for fusing . . . biometric technologies into advanced human identification systems to enable faster, more accurate, and unconstrained identification at great

The Supreme Court has not analyzed facial recognition software as it has tracking or magnification. But commentators have borrowed from the Court's language in other Fourth Amendment cases to build arguments for facial recognition that parallel those that the Court has offered for tracking and magnification.²³⁷ First, such commentators say, just as the magnification permitted in *Dow Chemical* simply enlarged images already visible to ordinary members of the public, so facial recognition uses for raw data only images taken from public settings.²³⁸ And one's facial appearance, as the Supreme Court noted in *United States v. Dionisio*, can hardly be characterized as private since, like one's voice, it is "constantly exposed to the public" and "[n]o person can have a reasonable expectation that . . . his face will be a mystery to the world."²³⁹ Thus, the argument goes, the government need not impinge on anyone's privacy to determine what he looks like or to use this publicly-available knowledge of his appearance to locate him on a street or among a group of people.

Proponents often provide a second related argument for leaving facial recognition unrestricted by the Constitution which, not surprisingly, mirrors the arguments invoked by the Court with respect to tracking and magnification. They argue that such technologies are nothing more than new, more effective incarnations of traditional and unquestionably acceptable law enforcement practices. Thus, says one commentator, facial recognition appears constitutionally unproblematic since using the "system is the equivalent of officers observing a crowd and comparing the faces in it to those in a criminal face book; it is just much faster and may be more accurate."²⁴⁰

distances"), at http://www.darpa.mil/body/newsitems/darpa_fact.html; see also Senior & Bolle, *supra* note 230, at 90 (noting that "[m]uch research effort around the world is being applied to expanding the accuracy and capabilities of this [face recognition technology]").

237. See, e.g., McCoy, *supra* note 77, at 480 n.67 (2002) (citing *Katz* and *Kyllo*, among other cases, to support the conclusion that "implementation of facial-recognition technology is not a search prohibited by the Fourth Amendment because it does not violate reasonable expectations of privacy").

238. Alexander T. Nguyen, *Here's Looking at You, Kid: Has Face-Recognition Technology Completely Outflanked the Fourth Amendment?*, 7 VA. J.L. & TECH. 2, ¶ 21 (Spring 2002), at http://www.vjolt.net/vol7/issue1/v7i1_a02-Nguyen.pdf (noting that the use of facial recognition technology "is almost certain to pass constitutional muster because there is neither a subjective nor an objective expectation of privacy in public spaces").

239. 410 U.S. 1, 14 (1973).

240. Kanya A. Bennett, Comment, *Can Facial Recognition Technology Be Used to Fight the New War Against Terrorism?: Examining the Constitutionality of Facial Recognition Surveillance Systems*, 3 N.C. J.L. & TECH. 151, 168 (2001); see also McCoy, *supra* note 77, at 488 ("The foundation of facial-recognition technology is similar to a police officer standing in a crowd with a stack of mug shots and comparing them to people who walk past him.").

There are also characteristics of facial recognition that make it privacy-enhancing, and these might appear to allay concerns that this technology runs afoul of the Fourth Amendment's proscription on investigations that are privacy-invasive. Most notably, many commonly used facial recognition methods—like other “biometric” technologies that identify people from biological characteristics—do not compare images; they compare measurements. Facial recognition technology frequently uses a “feature extraction” process²⁴¹ to take measurements of 80 or more nodal points on the face—such as the “upper ridges of the eye sockets, areas around the cheek bones, sides of the mouth, nose shape, and the position of major features relative to each other”²⁴²—and then uses algorithms to translate those measurements into an identifying record or “face print” that consists, not of a picture, but of a numeric string.²⁴³ With this record in its database, a facial recognition system then tests for a “match” by taking measurements from a person's face, creating another numeric template, and comparing the new numeric template to the one in its database—with the aid of an algorithm—to see if the degree of similarity between the two “templates” warrants a conclusion that the face it is observing matches the “face print” in its database.²⁴⁴ Because “biometric templates” of faces or fingerprints include only a very limited selection of data about any individual face or fingerprint, no one can reconstruct the appearance of a face or fingerprint from its numeric code, any more than one can reconstruct the contents of a whole novel from an identifying code that consists only in letters selected from specific positions in the text.²⁴⁵ Indeed, such lightning-fast automated

241. This process is normally treated as confidential by the company that produces the biometric process. NANAVALI ET AL., *supra* note 226, at 18.

242. *Id.* at 67.

243. As Nanavati et al. stress, biometric technologies generally do not make matches by using “an unprocessed image or recording of a characteristic.” Rather, they take the “raw biometric data” (for example, the record of a face or retina map) and then extract certain features of it to create a small file—called a “template”—which contains distinctive measurements that can then be compared to templates constructed at other times to see if they likely come from the same face or fingerprint (or whatever physiological characteristic is being used by the biometric process). *Id.* at 17–21; see also *Biometrics and the Future of Money: Hearing Before the Subcomm. on Domestic and Int'l Monetary Policy of the House Comm. on Banking & Fin. Servs.*, 105th Cong. 13 (1998) (statement of James L. Wayman, Dir. U.S. Nat'l Biometric Test Ctr., San Jose State Univ.) [hereinafter Statement of James L. Wayman] (“It is not the fingerprint that is encrypted on [a smart card used for biometric verification]. It is numbers coming from the fingerprint that are put in the code of the card.”), available at http://commdocs.house.gov/committees/bank/hba48784.000/hba48784_0f.htm.

244. NANAVALI ET AL., *supra* note 226, at 20 (noting that a comparison is deemed a match when the similarity—measured as a numeric “score”—exceeds a certain “threshold” number chosen by the system administrator).

245. See Statement of James L. Wayman, *supra* note 243, at 13 (noting that “[e]ven if [the] numbers [from a fingerprint] were sent to the FBI, the FBI could not reconstruct the fingerprint”);

comparisons between “face prints,” in which no human observer is involved,²⁴⁶ might strike many people as less invasive of privacy than having a police officer stare at faces in a line or a crowd to judge their similarity with a mugshot. It would not be surprising if courts recited such characteristics of facial recognition, and cited *United States v. Dionisio*,²⁴⁷ to hold that facial recognition in public falls entirely outside of the scope of the Fourth Amendment.

Such an analysis, however, ignores powerful reasons that some forms of facial recognition technology should be subject to Fourth Amendment limits. First, to the extent that facial recognition can easily be used to locate people in videotape footage or to retrace their movements, it would be subject to the Court’s caveat in *Knotts* that tracking might be constitutionally problematic when it is widespread and ongoing.²⁴⁸

Another possible basis for regulating facial recognition technology may be found in the Court’s decision in *Dow Chemical*.²⁴⁹ As noted earlier, the Court, in that decision, refused to classify as a Fourth Amendment “search” the use of a high-power map-making camera, but supported its conclusion by noting that the camera did *not* capture any “identifiable human faces.”²⁵⁰ Of course, video cameras supplemented by a facial recognition system not only might capture identifiable human faces—they are designed to do so—but also identify the faces they record.

But perhaps the most powerful reason for limiting facial recognition technology comes not from Fourth Amendment decisions on tracking and magnification, but from the Court’s vigilant defense of anonymity. While *Dionisio* noted correctly that a person cannot expect his face to “be a mystery

NANAVATI ET AL., *supra* note 226, at 19 (“An analogy would be to select a string of letters from a page by taking the 10th letter, 20th letter, 30th letter, and so on. You would have a string of characters that, in and of themselves, had no meaning and that could not be used to rebuild the original text.”).

246. Nanavati et al. point out that current methods of face recognition often do require the involvement of a human observer to verify that a machine-made match is accurate. NANAVATI ET AL., *supra* note 226, at 69. However, such an observer would only become involved in a small portion of the face recognition process (i.e., when the software indicates a match) and might one day be dispensable as the technology becomes more accurate. See *id.* (suggesting that facial-scan systems could be configured to narrow potential matches to 10 out of a possible 10,000 prior to any decision by a human operator); see also *infra* Part V for a discussion of how the lack of a human observer in an automated recording process might transform otherwise unconstitutional searches into “reasonable searches” permitted by the Fourth Amendment.

247. 410 U.S. 1 (1973).

248. See *United States v. Knotts*, 460 U.S. 276, 284 (1983) (“[I]f such dragnet-type law enforcement practices . . . should eventually occur, there will be time enough then to determine if different constitutional principles may be applicable.”).

249. *Dow Chem. Co. v. United States*, 476 U.S. 227 (1986).

250. *Id.* at 238 n.5, 239.

to the world,”²⁵¹ his identity often is. A person’s face does not identify him by name to all who see it, or provide observers with other personal information. If it did, authorities equipped with video cameras would have little need for facial recognition technology in the first place. Thus, as the Supreme Court recently noted in the First Amendment context, a person does *not* lose her right to retain her anonymity as soon as she shows her face.²⁵² Striking down a town ordinance that required all individuals to provide their names to a town before engaging in any door-to-door solicitation or canvassing, the Court squarely rejected the argument that anonymity is lost as soon as one appears in public. “The fact that circulators revealed their *physical* identities,” observed the Court, “[does] not foreclose our consideration of the circulators’ interest in maintaining their anonymity [since] . . . [i]n the Village, strangers to the resident certainly maintain their anonymity”²⁵³ Therefore, it is possible that even if Fourth Amendment protection is not triggered when the government records the photograph or “face print” of a person’s face, it will be triggered when investigators subsequently use facial recognition or other biometric technology to immediately acquire otherwise difficult-to-acquire identifying information about an unknown individual.

Of course, when we act in public we reveal not only our appearance, but often our identity as well. We respond to our names and show our drivers’ licenses or other identifying documents to security guards and store clerks. Airport staff typically verify our identities, usually by glancing at photo identification, before allowing us to check in luggage or proceed to an airport gate. And it is not only facial recognition devices that could recognize us in a crowd, but also an acquaintance or an investigator holding a picture of us. Consequently, when one looks narrowly at a particular activity on a given day, one might argue that our anonymity might have been taken away in that circumstance as much by a chance encounter with a friend or acquaintance as by advanced technology. But what such an observer could not do is remove all opportunities for anonymous or private action in a substantial portion of public space. While an acquaintance might happen to find us in a crowd of thousands at a protest rally, he cannot be relied upon to do so each time we attend such an event, and an airport staff member or security guard is unlikely to remember our identities—or that of the many other people he checks in—after he has verified that we are who we claim to be.

251. *United States v. Dionisio*, 410 U.S. 1, 14 (1973).

252. *Watchtower Bible & Tract Soc’y of N.Y., Inc. v. Stratton*, 536 U.S. 150, 166–67 (2002) (rejecting the Sixth Circuit’s basis for refusing to protect anonymity).

253. *Id.* at 167 (emphasis added).

Such concerns about loss of anonymity do not disappear simply because most biometric devices compare numeric codes rather than identifiable images. In the first place, some methods of representing faces for purposes of facial recognition may require face prints to contain information that would allow investigators to reconstruct a person's appearance. For example, instead of measuring well-known facial features, the "eigenface" method encodes a face's global appearance by representing it as a weighted mix of certain face patterns in a database of grayscale images. One analysis notes that in contrast to geometry-based methods, which can match faces "without any need for actual facial images at the comparison point," matching in the eigenface method "is done on a pixel-by-pixel basis."²⁵⁴ Even when the code in a "face print" cannot be used by the police to reconstruct the appearance of someone's face, when used in conjunction with facial recognition technology, it can allow them to pick a face out of a crowd, or out of video footage, and to learn a great deal about the person to whom the face belongs. Even without a photograph of a person, an official might quickly eliminate his anonymity with the aid of an identifying code.

Facial recognition is not the only biometric technology that can make video surveillance a much more potent tool for invading individuals' privacy. To be sure, apart from a person's face, few physical characteristics or personal traits commonly used in biometrics are likely to appear in a video image. Video cameras are ill-suited to capture useful data about a person's fingerprints,²⁵⁵ the three-dimensional geometry of her hand,²⁵⁶ or the distinctive physical attributes of her eyes, such as the vein patterns in her retinas²⁵⁷ or the structure of her irises.²⁵⁸ Without audio capacity, cameras

254. Stephen Cass & Michael K. Riesenman, *Improving Security, Preserving Privacy*, IEEE SPECTRUM ONLINE, at <http://www.spectrum.ieee.org/WEBONLY/publicfeature/jan02/secure.html> (last visited Mar. 24, 2004); see also Michael Bromby, *Computerised Facial Recognition Systems: The Surrounding Legal Problems* 10 (2000) (unpublished L.L.M. dissertation, University of Edinburgh), available at <http://cbs1.gcal.ac.uk/law/users/~mbro/documents/LLMDissertation.pdf> (stating that only 40 face patterns "are required to reconstruct a 99% accurate composite face of the initial subject due to the limited number of differences between every existing and possible face"); Xiaou Tang & Xiaogang Wang, *Face Sketch Recognition*, 14 IEEE TRANSACTIONS ON CIRCUITS & SYSTEMS FOR VIDEO TECH. 50, 52 (2004) (stating that "a face image can be approximately reconstructed using a weighted combination of the eigenfaces").

255. Fingerprints used for biometric matches are generally taken with specialized readers that require a person to place his finger on a surface called a "platen." Measurements of distinctive features of the fingerprint are then taken with the aid of chip-based cameras or ultrasonic imaging. NANAVATI ET AL., *supra* note 226, at 46–47.

256. Hand geometry is currently the most widely-used biometric in the travel and immigration industry. *Id.* at 229. It relies on measurements based on three-dimensional images of the back and sides of the hand. *Id.* at 100–01.

257. The retina is "the surface on the back of the eye that processes light" that has entered through the pupil. *Id.* at 106. Each retina has a distinctive pattern of blood vessels, which can be

are of course also unable to record or identify the distinctive features of a particular person's voice.²⁵⁹ In general, biometrics systems using these physical features use them not for identification, but for verification of a claimed identity. Before letting someone into a secured building, or into confidential computer files, a security system might ask the would-be entrant for a biometric identifier (like a fingerprint or iris scan), not to determine his name or any other personal information, but only to verify that he is authorized to enter.²⁶⁰

To the extent that such verification systems save any identifying information tying particular people to particular places or activities, they might have the consequence of making existing surveillance systems, such as cameras, much more invasive. If fingerprinting or iris scanning devices frequently record when a particular person has used a specific ATM or entered a specific building, then such data could conceivably aid a video search of that person's movements, in the same way that Intelligent Highway Systems or phone company records might aid such a search by providing information about the location of a person's car or cell phone. Indeed, biometric technology could allow for more inescapable tracking, because while your car or your cell phone can be used by someone else, it is virtually impossible for another person to use your fingerprint or retina.²⁶¹ And unlike

mapped with the aid of infrared imaging and used as the basis for assigning a person a unique biometric code. *Id.* at 108–09. It is extremely accurate, and produces very few “false matches.” *Id.* at 110.

258. The iris is the colored membrane that surrounds the pupil of the eye, and each iris is marked by highly distinctive patterns (in fact, even in a single person, the iris of the left eye differs in structure from that of right eye). *Id.* at 80. Like a retina scan, an iris scan uses infrared imaging to acquire data on the iris. *Id.* at 78.

259. Voice scanning devices measure distinctive aspects of the way someone speaks. *Id.* at 87–93. According to Nicholas Orlans, voice recognition technologies under development could allow analysts to locate specific speakers on a tape instead of “listening to weeks or months of general archives” and might help “link voices to identities on wiretap data” used by law enforcement. Orlans, *supra* note 27 at 71, 83.

260. As many writers on biometrics note, such a verification system differs from an identification procedure in that its task is not to answer the question “Who am I?” but rather the question “Am I who I claim to be?” See, e.g., NANAVATI ET AL., *supra* note 226, at 12–13.

261. See John D. Woodward, *Biometric Scanning, Law & Policy: Identifying the Concerns—Drafting the Biometric Blueprint*, 59 U. PITT. L. REV. 97, 100–01 (1997) (noting that “[t]he unique advantage of biometrics is that it bases identification on an intrinsic aspect of a human being,” which, unlike keys or passwords, cannot be “lost, duplicated, stolen, or forgotten at home”). While it is conceivable that people might find ways to imitate such biometric characteristics, it is much harder to do so than to steal passwords or PINs, and “liveness” testing can help ensure that the biometric data is coming from a live human being. See Valorie S. Valencia, *Biometric Liveness Testing*, in WOODWARD ET AL., *supra* note 27, at 139–49 (discussing liveness testing, which determines whether a “biometric sample . . . came from . . . the live human being who was originally enrolled in the [biometric] system”); Robyn Moo-Young, “Eyeing” the Future: Surviving the Criticisms of Biometric Authentication, 5 N.C. BANKING INST. L.J. 421, 430, 434, 450 (2001) (noting that iris identification can measure “physiological response to light” and thus verify that

facial recognition technology, which might be thwarted by changes in environment or appearance, biometric techniques such as iris and retina scans, and to a lesser extent fingerprint matching, are almost impossible to deceive or circumvent.²⁶²

C. Detection

Another kind of caselaw also casts doubt upon the *Katz* framework, and it deals with the very threat that *Katz* was meant to address: the danger that police will use modern technology to somehow circumvent physical barriers that are relied upon to keep information private. As I have noted above, courts that refuse to treat public surveillance as a “search” sometimes explain this result by underscoring how such surveillance differs from the paradigmatic electronic search in which investigators somehow look or listen through a wall or window.²⁶³

But in the decades since *Katz*, difficult questions have arisen, both about whether detection technologies are generally “searches” under the Fourth Amendment and about how much weight courts can continue to place on the distinction between “see through” technologies, which presumably upset reasonable expectations of privacy, and mere “enhancements” of visual observation, which presumably do not.

Some modern detection devices, to be sure, present little problem for the *Katz* paradigm. Most people agree, for example, that airport officials are conducting Fourth Amendment searches when they use X-ray devices or so-called millimeter scanning devices.²⁶⁴ While clothing and luggage are usually impermeable to visible light (largely to cloak what lies underneath or inside), X-rays and millimeter radiation pass right through these barriers,

“the pupil is in fact moving,” and that fingerprint readers can recognize a “distressed finger,” which may be a sign that someone is trying to force another person to provide unauthorized entry).

262. See, e.g., *Orlans*, *supra* note 27, at 93 (noting that iris recognition tests have been “almost flawless,” and that the odds of two irises generating a false match are theoretically 1 in 1.2 million); see also *Woodward*, *supra* note 261, at 100 (noting that the only three features commonly used in biometrics that are “considered truly consistent and unique” are “the retina, the iris, and fingerprints”); *NANAVATI ET AL.*, *supra* note 226, at 58 (noting that the fingerprint is a “highly distinctive identifier” and that the iris and retina are even more distinctive).

263. E.g., *Dow Chem. Co. v. United States*, 476 U.S. 227, 239 (1986).

264. See, e.g., *United States v. Haynie*, 637 F.2d 227, 230 (4th Cir. 1980) (“[I]t is clear that the officer’s examination of Handshaw’s briefcase by means of an X-ray scanner was a search within the meaning of the Fourth Amendment.”); Charles J. Murray, *Beyond the Metal Detector: Engineers Seek Next Steps in Security Technology*, ELECTRONIC ENGINEERING TIMES, Sept. 17, 2001, at 42 (describing how millimeter scanning devices also allow investigators to see through barriers); see also Alyson L. Rosenberg, *Passive Millimeter Wave Imaging: A New Weapon in the Fight Against Crime or a Fourth Amendment Violation?*, 9 ALB. L.J. SCI. & TECH. 135, 140–52 (1998) (discussing the passive millimeter wave imager’s ability to detect concealed weapons and Fourth Amendment concerns related to such law enforcement technology).

allowing investigators with the right equipment to view what is on the other side and conduct the equivalent of an “electronic strip search.”²⁶⁵

But unlike the detection technologies described above, which can provide a vivid picture of practically everything an individual is hiding in a container or underneath a coat or shirt, many detection devices signal only the presence or absence of a particular substance or object with distinctive physical properties. The “magnetometers” that travelers typically have to pass through at airports, for example, detect only metals. They detect disturbances in the earth’s magnetic field and sound an alarm only after detecting the sort of disturbance caused by a metal object of, or above, a certain mass.²⁶⁶

The same basic mechanism is at work in many new, highly-sophisticated instruments for detecting weapons or illegal drugs.²⁶⁷ Many of these devices sense the presence of particular materials by reading magnetic or chemical “signatures.” One such device, for example, is a more refined version of a metal detector. It “measures what objects do to the earth’s magnetic field,” but instead of simply detecting the presence or absence of metal, it compares the measurements of magnetic field disturbance to “known signatures of weapons of similar shape, mass and density to determine the likelihood that the object is a weapon” of a particular kind.²⁶⁸ Another device, called the “Gun Tracker” scans people from a distance.²⁶⁹ When it detects a possible weapon on someone’s person, it triggers a video camera, which then follows the suspicious individual and places a red dot at the location on the person’s image where the Gun Tracker has located the potential weapon.²⁷⁰

Other devices use “chemical signatures” to detect explosives or narcotics. Perhaps the most familiar “chemical signature” detector is the trained bomb- or drug-sniffing dog. But scientists have recently developed many new mechanical “sniffing” devices. A machine called “the Senter,” for example, uses high-speed gas chromatography to quickly search the air

265. See, e.g., Paul Marks, *Scanner Takes It Off, Takes It All Off; Airport Security Officials Attracted to “Strip-Search” Technology*, HARTFORD COURANT, Mar. 28, 2002, at A1 (describing a new backscatter X-ray device, the Rapiscan Secure 100, and noting that it “is best described as a hands-off strip search”).

266. David A. Harris, *Superman’s X-Ray Vision and the Fourth Amendment: The New Gun Detection Technology*, 69 TEMP. L. REV. 1, 46–47 (1996).

267. Roberto Iraola, *New Detection Technologies and the Fourth Amendment*, 47 S.D. L. REV. 8, 9–12 (2002).

268. *Id.* at 10.

269. Leigh Fenly, *Invasion of the Body Searchers: The Latest in Security Technology Has Its Eyes on Would-Be Bad Guys*, SAN DIEGO UNION-TRIB., Aug. 30, 2000, at F1.

270. *Id.*

around a suspect or his baggage for even the slightest molecular traces of narcotics.²⁷¹ Other devices “emit puffs of air that pick particles off [airline travelers’] clothing” for instantaneous chemical analysis,²⁷² or detect explosives on the surface of luggage by firing energized neutrons or lasers at it in order to cause a “signature” reaction that will identify even small amounts of explosives or other chemicals of interest.²⁷³ Researchers have also been developing “smart dust”—tiny silicon chips, to be dispersed in the air or blended into the paint on the surface of a building or vehicle, that can detect and identify deadly biological or chemical agents nearby.²⁷⁴

At first glance, it may seem as though these devices provide grounds for limiting constitutional privacy protections rather than extending them. Devices focused on drugs or explosives, for example, have made it plausible to think scientists might be able to manufacture devices that can directly “sense” illegal, or at least highly suspicious, activity and in this way spare police the intrusive information gathering that would otherwise be necessary before determining which house or container to search. According to Arnold Loewy, such a technique of searching—epitomized by high-tech chemical detectors and by marijuana-sniffing dogs—approximates the kind of search police would use in a more perfect crime-fighting regime where nonintrusive technology could automatically distinguish criminal from innocent activity. In Loewy’s law enforcement utopia:

[E]ach policeman would be equipped with an evidence-detecting divining rod. He would walk up and down the streets and whenever the divining rod detected evidence of crime, it would locate the

271. Peter Joseph Bober, *The “Chemical Signature” of the Fourth Amendment: Gas Chromatography/Mass Spectrometry and the War on Drugs*, 8 SETON HALL CONST. L.J. 75, 77 (1997). As Bober explains, “[t]he Sensor filters a volume of air and screens out smoke, auto exhausts, and millions of other compounds, and identifies the amounts of cocaine, heroin, or methamphetamine that are present.” *Id.*

272. Andrew Garber, *New Airport Gadgets Strip, Sniff, Scan*, SEATTLE TIMES, Oct. 23, 2001, at A1.

273. See Eric J. Lerner, *Photonics Promises Improved Security: Lasers, Optical Scanners, and Other Optoelectric Technologies May Enhance Protection of Critical Locations Against Acts of Terrorism—But There Are Tradeoffs*, LASER FOCUS WORLD, Dec. 2002, at 45 (describing a system that analyzes “the light produced when tiny amounts of explosive are detonated by a laser pulse”); *Market Call: Tom Pascoe, Maverick of the Morning: Hi-Tech Bomb Detecting* (CNNfn television broadcast, Oct. 30, 2002) (interviewing the CEO of the company that produces the MiniSenzor, a product that identifies the chemical signatures of objects by bombarding them with neutrons and then reading the gamma waves consequently produced by the object, the character of which will be “unique for every element of the periodic table”), transcript available at http://www.hienergyinc.com/press/CNNFN%20Market%20Call_103002.pdf.

274. See *Tiny Smart Dust Particles Capable of Detecting Bioterrorist and Chemical Agents*, SPACE DAILY, Sept. 9, 2002, available at <http://www.spacedaily.com/news/terrorwar-02r.html>; Seth Hettena, *San Diego Scientists Applying Research to Homeland Security*, N. COUNTY TIMES, Sept. 6, 2002, available at <http://www.nctimes.net/news/2002/20020906/60225.html>.

evidence. First, it would single out the house, then it would point to the room, then the drawer, and finally the evidence itself. Thus, all evidence of crime would be uncovered in the most efficient possible manner, and no innocent person would be subject to a search. In a real society (such as ours), the fourth amendment serves as an imperfect divining rod.²⁷⁵

The same year that Loewy published this article, the Supreme Court agreed that a canine sniff revealing only the presence of contraband was not the kind of investigation the Fourth Amendment was meant to constrain. In *United States v. Place*, the Court found—in response to a traveler’s complaint about a warrantless use of a drug-sniffing dog to examine his luggage—that there was no invasion of a Fourth Amendment privacy right because “the sniff discloses only the presence or absence of narcotics, a contraband item.”²⁷⁶ The Court stressed that the canine sniff was *sui generis*.²⁷⁷ It was unique in that it targeted only the guilty and left legitimate privacy interests unharmed. The following year, in *United States v. Jacobsen*,²⁷⁸ the Court found another real-life example of Loewy’s “evidence detecting rod” in the chemical tests used by field agents to determine if a white powder was cocaine. Federal Express employees had found the powder inside a damaged package sent by defendants and turned it over to police.²⁷⁹ As it had done with respect to the canine sniff in *Place*, the Court in *Jacobsen* stressed that “[a] chemical test that merely discloses whether or not a particular substance is cocaine does not compromise any legitimate interest in privacy.”²⁸⁰

Not surprisingly, courts and commentators have since taken note of other focused search techniques that might fit the same model. In his dissent in the Court’s recent *Kyllo* decision, Justice Stevens, the author of the Court’s decision in *Jacobsen*, noted that the rule in *Place* should apply not only to dog sniffs, but also to devices that “detect [only] the odor of deadly bacteria or chemicals for making a new type of high explosive.”²⁸¹ The Sensor and other devices, one might argue, fit this description. After

275. Arnold H. Loewy, *The Fourth Amendment as a Device for Protecting the Innocent*, 81 MICH. L. REV. 1229, 1244 (1983).

276. *United States v. Place*, 462 U.S. 696, 707 (1983).

277. *Id.* (“In these respects, the canine sniff is *sui generis*. We are aware of no other investigative procedure that is so limited both in the manner in which the information is obtained and in the content of the information revealed by the procedure.”).

278. *United States v. Jacobsen*, 466 U.S. 109, 124 (1984).

279. *Id.* at 111. The police themselves could not have constitutionally investigated the package, but the Fourth Amendment bar against such searches did not apply to private companies acting on their own initiative, as Federal Express did here before contacting the police. *Id.* at 114–15.

280. *Id.* at 123.

281. *Kyllo v. United States*, 533 U.S. 27, 47–48 (2001).

collecting a sample of the air around a person, or the matter on his clothing, such devices determine only if drugs or explosives are present. And one writer examining facial recognition technology, Alexander Nguyen, has suggested that the rule in *Place* and *Jacobsen* might apply to facial recognition technology as well, at least where it destroys the anonymity *only* of those who police have determined are criminals or have connections to terrorist groups:

Facelt [a well-known device for face recognition] generates a face print and compares it to files in its database of wanted criminals—and, according to company officials, discards the computerized print from its memory if there is no match. In this way, all Facelt really does is answer a simple question: Is the individual being scanned a criminal? . . .

Indeed, Facelt very closely resembles metal detectors at airports or dog sniffs that the Court has held constitutional in *United States v. Place* where no search warrant or probable cause was present, or a test by law enforcement officials of white powder to determine whether or not it was cocaine as opposed to sugar or talcum powder which the [C]ourt held constitutional in *United States v. Jacobsen*.²⁸²

Such analogy to *Place* or *Jacobsen* is attractive because it suggests a way in which vigorous protection of privacy might be reconciled with increased law enforcement vigilance against hard-to-detect threats. Yet there are a number of reasons that courts should be extremely cautious in extending the *Place* and *Jacobsen* model, especially in the case of video surveillance. First, it is rare that devices can single out *only* illegal activity or materials. As Arnold Loewy stresses, even “so innocuous a device as a magnetometer cannot distinguish permissible metals (coins, keys, etc.) from impermissible ones (guns, knives, etc.).”²⁸³ Partly for this reason, courts have invariably held that use of magnetometers at airports or federal buildings is a search.²⁸⁴

282. Nguyen, *supra* note 238, ¶¶ 23–24. Nguyen resists this conclusion and argues for a “re-conceptualization of the Fourth Amendment” that will protect citizens from unconstrained use of such biometric technology. *Id.* ¶ 55. But his analogy to *Place* and *Jacobsen* illustrates how the Supreme Court’s recent jurisprudence on detection technology might weaken opportunities for anonymity or unmonitored activity in public places.

283. Loewy, *supra* note 275, at 1246.

284. See *United States v. Albarado*, 495 F.2d 799, 803, 805 (2d Cir. 1974) (classifying a magnetometer walk-through as a search and noting that “although calibrated supposedly to be activated by a mass of metal approximating a .25 calibre pistol, often [it] is activated by car keys, ladies sewing scissors, briefcase hinges and latches, and the like”); *United States v. Epperson*, 454 F.2d 769, 770 (4th Cir. 1972) (holding that the use of a magnetometer on a person boarding an aircraft is a search within the meaning of the Fourth Amendment).

Second, a surveillance device will not necessarily cease to intrude upon the privacy of the innocent even if it does detect only contraband. Particularly when the device is extremely sensitive and picks up molecular traces of a chemical, it might find traces of narcotics not only on someone who possesses drugs, but also on someone who had incidental contact with the drug possessor.²⁸⁵ As Peter Bober notes, a police officer using the Sentor to sample the air around a person might find trace amounts of narcotics in the environment not because that person possesses drugs, but because the police officer herself has unknowingly carried trace amounts of narcotics on her own person after conducting an earlier drug bust.²⁸⁶ Many devices also occasionally give “false positives.” They signal the presence of drugs or explosives even when there are none. For example, after shutting down San Francisco International Airport and searching unsuccessfully for a traveler who tested positive for explosives, but was mistakenly allowed by a guard to proceed, authorities noted that the substance detected was probably fertilizer, which has a chemical signature identical to that of certain explosives.²⁸⁷

There is a third reason why surveillance techniques that pick out only illegal activity might harm the privacy interests of innocent people, even when functioning perfectly. As Michael Adler points out, a search that pierces a house or container wall only to uncover illegal activity can severely undermine the confidence that people have in homes and other private environments more generally.²⁸⁸ Even when the activity they wish to shield is entirely innocent, people may be justifiably unnerved by the state’s ability to effortlessly monitor and gather information from environments that are supposed to serve as sanctuaries for freedom.²⁸⁹

Such skepticism about targeted or noninvasive technologies was clearly evident in the Court’s recent decision in *Kyllo*, in which it held that the police engaged in a Fourth Amendment “search” when they spied on the inside of a private residence with a thermal imager.²⁹⁰ To be sure, such a device is in some ways similar to an X-ray or millimeter scanning device. It allows police to “see” in heat measurements things they cannot see with visible

285. Bober, *supra* note 271, at 77.

286. *Id.* at 109–10.

287. Ray Delgado, *Back to Business as Usual for SFO: But FBI Continues Investigation on the Passenger Who Got Away*, S.F. CHRON., Jan. 31, 2000, at A10.

288. Michael Adler, *Cyberspace, General Searches, and Digital Contraband: The Fourth Amendment and the Net-Wide Search*, 105 YALE L.J. 1093, 1110 (1996).

289. *Id.* (“[I]nasmuch as targets know that the search could potentially be directed toward unpopular but noncriminal activities, the search may impose a chilling effect on the exercise of such activities.”).

290. *Kyllo v. United States*, 533 U.S. 27, 40 (2001).

light, and therefore allows them to “see” people or things that emit heat from the other side of a wall.²⁹¹

But forward looking infrared (FLIR) devices like that used in *Kyllo* do not provide anything approaching a vivid picture. They show only significant differences in temperature, and in most cases, seem to uncover little beyond the possession of high-intensity lamps of the kind needed to grow marijuana indoors. As the dissenting opinion in *Kyllo* stressed, the surveillance in that case was conducted with “a fairly primitive thermal imager,” which merely collected “from the exterior surfaces of [Kyllo’s] home” heat measurements showing only “relative differences in emission levels, vaguely indicating that some areas of the roof and outside walls were warmer than others.”²⁹²

Nonetheless, the Supreme Court squarely rejected the arguments that such technological crudeness made the Fourth Amendment inapplicable. Just as metal detectors might invade the privacy of people carrying coins or other entirely innocent metal objects, FLIR devices might reveal sources of heat that have nothing to do with drug possession. As Justice Scalia noted, it “might disclose, for example, at what hour each night the lady of the house takes her daily sauna and bath.”²⁹³ More important for the Court was an argument akin to Adler’s argument that even unintrusive searches focused narrowly on criminal activities can undermine the sanctity of a private environment and the security that people feel in it. As Scalia stressed, it did not really matter whether the FLIR revealed particularly intimate details: “In the home . . . all details are intimate details.”²⁹⁴ To let the state surveil this environment unannounced and without a warrant would weaken the protection traditionally afforded to this most private of all environments.

While *Kyllo* emphasizes the integrity and historical importance of the home in Fourth Amendment jurisprudence, its position is similar to the positions that other commentators and Justices have taken against uncritically

291. See *id.* at 29–30 (“The imager . . . operates somewhat like a video camera showing heat images.”).

292. *Id.* at 41–43 (Stevens, J., dissenting). Some lower courts had also given another reason to conclude that the use of a FLIR device was not a search—namely, that the device constructed pictures from “waste heat,” which is no more internal to the house or unavailable for others’ inspection than garbage left by the side of a curb (which, as the Court held in *California v. Greenwood*, 486 U.S. 35, 40–41 (1988), is not the subject of a “reasonable expectation of privacy”). See, e.g., *United States v. Pinson*, 24 F.3d 1056 (8th Cir. 1994); *United States v. Penney-Feeney*, 984 F.2d 1053 (9th Cir. 1993). Such arguments would probably have been of little aid in exempting FLIR from the scope of the Fourth Amendment, though, if thermal imagers could (like X-ray devices) provide police with a detailed portrait of what goes on inside the home the way passive millimeter radiation can provide information about what is underneath clothing or inside containers.

293. *Kyllo*, 533 U.S. at 38.

294. *Id.*

applying *Place* to permit “dog sniff” type surveillance in public spaces as well. Even for those who do not possess, or plan to possess, any drugs, constant and visible use of police dogs may dampen the freedom they feel in public spaces. Thus, even as he compares dog sniffs to “divining rods” that reveal only criminal activity, Arnold Loewy emphasizes that he does not endorse the “carte blanche use of marijuana-sniffing dogs,” in part because of the effect that even errorless dogs would have on innocent people: “[T]he very act of being subjected to a body sniff by a German Shepherd may be offensive at best or harrowing at worst to the innocent sniffer.”²⁹⁵ In his dissent in *Jacobsen*, Justice Brennan likewise warned that “under the Court’s analysis in [*Place* and *Jacobsen*], law enforcement officers could release a trained cocaine-sensitive dog . . . to roam the streets at random,” or put people and houses under the constant watch of machines that detect illicit chemicals, something which would give our society a resemblance to authoritarian societies that refuse to trust their citizens with any freedom.²⁹⁶

Such considerations provide reason to extend Fourth Amendment safeguards even to detection technologies that purportedly uncover only the guilty. They also apply with just as much force to surveillance technologies that purportedly reveal only that which is already visible. Carte blanche use of cameras may undermine freedom in the public sphere as much as carte blanche use of drug-sniffing dogs. Indeed, cameras reveal even more than a canine sniff and, unlike a dog, a camera can record an ongoing tape of one’s activities for later investigation. Like chemical testing devices, facial recognition devices are also plagued by false positives. Unlike iris scan and retina scan devices, which rarely make the mistake of matching different people, facial recognition in uncontrolled settings currently does so with great frequency.²⁹⁷ As biometrics researcher James Wayman observes, such technology produces false alarms and will sometimes identify innocent people as terrorists.²⁹⁸ This does not mean that such technologies should never be used, but it does mean that even if they observe people only in public spaces, state-operated camera systems, like imperfect detection technologies, should be included within the scope of the Fourth Amendment so that courts may test their reasonableness and thereby assure that whatever damage they do to privacy is both necessary and as limited as possible.

295. Loewy, *supra* note 275, at 1246–47.

296. *United States v. Jacobsen*, 466 U.S. 109, 138 (1984) (Brennan, J., dissenting).

297. See *supra* notes 227–30 and accompanying text.

298. See Garber, *supra* note 272 (quoting Wayman and noting that, despite false alarms, Wayman finds face recognition useful for culling passengers at airport terminals down to a short watch list that can be more easily checked for ties to terrorism).

There is also another reason that courts' and commentators' skepticism about exempting detection technologies from Fourth Amendment coverage should be extended to video surveillance. Imagine a public camera system which, instead of filming everybody all of the time, was activated only when a metal detector or some "magnetic signature" detector signaled that a person walking on a street near a high security building had a metal object the size of a hand gun. As noted above, a device called a "Gun Tracker" operates in this way.²⁹⁹ It trains a camera on a person, and a red dot on the location of the potential weapon, only after detecting a magnetic signature that might belong to a dangerous object. It is hard to resist the conclusion that, because government use of an ordinary metal detector counts as a search, the activation of such a camera would count as a search as well. But such a surveillance system would intuitively be far less invasive of privacy than one that filmed people everywhere whether or not they carried a gun-sized metal object. To be sure, the latter camera system would be less intrusive than the former in one respect. It would not tell an observer whether the object hidden in a person's pocket or zippered bag were made of metal or some other material or provide information about the mass and shape of the object. But in every other respect, a pervasive, constantly operating network of public cameras would be more damaging to an individual's sense of privacy than would one that is activated only upon detection of potentially dangerous objects or substances.

III. Beyond the *Katz* Test: Protecting Privacy in Public Places

A. *Privacy Interests in Public Space*

While courts have hinted that widespread tracking or videotaping of people's movements might violate the Fourth Amendment, they have said little about why or how such a conclusion squares with the jurisprudential framework inherited from *Katz*.³⁰⁰ If, as the Supreme Court held in *Knotts*, a single individual has no reasonable expectation that his movements will remain shielded from intensive scrutiny,³⁰¹ then it is hard to understand why (under the *Katz* test) he would have any more right to such an expectation of privacy in a world where the government routinely tracks many citizens' movements. Where ubiquitous public cameras, electronic tollways, and cell phones regularly capture people's locations and movements, an individual

299. See *supra* notes 269–70 and accompanying text.

300. See *supra* notes 39–40 and accompanying text (explaining that it is not a search when the government observes something a person exposes to the public).

301. See *United States v. Knotts*, 460 U.S. 276, 285 (1983) (holding police use of an electronic tracking device to track the movement of a drum constitutional).

would have less reason to be surprised or shocked that police can figure out exactly where he is, where he has been, and what he has done.³⁰² To be sure, mass video surveillance of law-abiding citizens does seem intuitively akin to the unrestricted house-to-house searches and unbounded fishing expeditions that the Fourth Amendment was clearly meant to eliminate. But neither *Katz* nor the cases that follow it explain how such dragnet techniques can violate people's reasonable expectations of privacy in open, easily observed areas where they can have no such reasonable expectations.

The answer to this puzzle lies largely in recognizing that people *do* have important privacy interests in public places, and that mass video surveillance systems can threaten them much more severely than law enforcement techniques of the past. The *Katz* decision and cases applying it have failed to carefully delineate and protect the privacy of public spaces, but this may be because *Katz* and its progeny were focused on an entirely different sort of threat. As I have emphasized in Parts II and III of this Article, these cases focused on addressing the problems created by what one might call "see through" surveillance. They aimed to patch up the breach in Fourth Amendment privacy protection created when science revealed and allowed people to exploit the fact that various physical phenomena—such as heat, radio waves, and millimeter waves—could carry information about "the privacies of life" through the barriers and doors that were supposed to keep outsiders from seeing or hearing inside.

Mass video surveillance or tracking is similar in that it too gives investigators a way to intrude upon the privacies of individuals' lives without physically entering their private residences. But it does so through a fundamentally different mechanism than X-ray or infrared devices. Instead of giving investigators a kind of unguarded pathway into people's private homes and conversations, it gathers raw material for detailed archives and profiles of their lives from the outside world itself. It takes advantage of the fact that evidence of people's private lives—personal beliefs, interests, activities, psychological or medical conditions, the states of family and romantic relationships—does not exist only behind physical barriers. While a public space might seem like a poor location for people to engage in private or personal activities, they often have little choice. When entering the office

302. One way to understand this problem is as an example of the general problem that characterizes the "subjective expectation" prong of the *Katz* test: namely, the government can make even the deepest violations of privacy expected by announcing them in advance. See *infra* Part IV. This is how one writer responds to the discussion in *Knotts* that 24-hour surveillance would merit a different treatment. See Philip H. Marcus, Note, *United States v. Knotts—'A Traveller's Advisory for 1984,'* 45 U. PITT. L. REV. 741, 770 (criticizing the *Knotts* Court for "inject[ing] its own subjective view of what society should deem as reasonable expectations of privacy in an automobile" and for choosing to discount the privacy concerns presented by modern surveillance technology until a more serious problem develops).

of a psychiatric or other medical specialist, they provide clues about their mental or physical condition. When examining an item of interest in a store window, they reveal evidence of their personal interests to anyone who might be observing them. Moreover, at least in an open society, couples and families do not feel obligated to remain tight-lipped and stone-faced in a street or open-air cafe. They show warmth, frustration, and other emotions that they do not intend to put on public display for the rest of the world or for public officials.

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. Such records present a deep threat to core liberty and privacy interests in a number of ways.

First, camera systems that capture all aspects of our public lives are likely (for the reasons given above) to sweep in some important elements of our "intimate" lives: elements of a person's medical condition, for example, or about personal relationships. According to many scholars, such intimate activities are precisely what privacy rights exist to protect. They exist, says James Rachels, to guard against the disclosure of "the sort of intimate fact about you that it is not appropriate for strangers or casual acquaintances to know."³⁰³ Video surveillance circumvents this safeguard by making an anonymous camera operator privy (in some degree) to facts that we would otherwise reveal only to our doctor, therapist, or family member. As Charles Fried argues, privacy "forms the necessary context for the intimate relations of love and friendship," and "where any intimate revelation may be heard by monitoring officials, it loses the quality of exclusive intimacy required of a gesture of love or friendship."³⁰⁴ Second, even where camera networks do not capture such intimate facts, they threaten core privacy interests. By severely undercutting our informational privacy—that is our ability to withhold certain facts about ourselves from others—such surveillance undermines one of the central conditions of personal autonomy in modern

303. James Rachels, *Why Privacy is Important*, in PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 290, 298 (Ferdinand David Schoeman ed., 1984).

304. Charles Fried, *Privacy [A Moral Analysis]*, in PHILOSOPHICAL DIMENSIONS OF PRIVACY, *supra* note 303, at 203, 216. For other arguments that justify privacy rights as means for safeguarding intimacy, see JULIE C. INNESS, *PRIVACY, INTIMACY, AND ISOLATION* (1992); Tom Gerety, *Redefining Privacy*, 12 HARV. C.R.-C.L. L. REV. 233, 234 (1977); Robert S. Gerstein, *Intimacy and Privacy*, 89 ETHICS 76 (1978).

societies. We are not, of course, able to mandate what people will think about what we say and do. Nor can we force others to avert their eyes when they see us. But, by taking account of others' presence and taking advantage of the many opportunities that modern life offers for anonymous or private action, we can "manage" this image and exert significant control over the appearance we present to others.

This autonomy is valuable for many individuals as an end in itself, but it is also valuable as an essential aid to many other core individual interests, most notably the interest in finding a way of life that fits one's needs and values. As Alan Westin has observed, individuals need environments for "sheltered experimentation" where they can address vulnerabilities they would rather not reveal to others and where they can explore interests and think through ideas that might be at odds with their public persona or with expectations of acquaintances, friends, or public officials.³⁰⁵ While the home provides the most obvious site for such "sheltered experimentation," it is not the only such site and is in many circumstances not the most important site. On the contrary, many of the resources essential for individuals to address vulnerabilities or to rethink existing ideas are available only if they venture into public life, to places such as libraries, religious centers, clinics, or stores. And we are used to being able to access these resources without the rest of the world, or public authorities, tracking our every use of them.³⁰⁶

Third, even where a person does not worry about a particular action being observed in isolation, such actions may reveal private thoughts or goals when viewed in the aggregate. For example, an individual might have a confidential career ambition, an idea for a novel, or a deep anxiety about certain issues, the nature of which will become clear only to an observer who can collect various pieces of evidence of a person's life and put them together in a way that would be impossible outside a world of general video surveillance. In the past, the best place to get access to a comprehensive picture of a person's interests was his home, where one might find records pertaining to many different aspects of his family life, work life, health, and

305. See Alan F. Westin, *Science, Privacy, and Freedom: Issues and Proposals for the 1970's*, 66 COLUM. L. REV. 1003, 1023-24 (1966) (stating that "sheltered experimentation" is crucial to a sense of personal autonomy).

306. Indeed, federal law protects against agencies receiving unnecessary access to records on our video rentals. Video Privacy Protection Act, 18 U.S.C. § 2710 (2000). Various state laws also protect against monitoring of library records. See, e.g., N.Y. CIV. PRAC. L. & R. § 4509 (McKinney 1992). These laws assume that protecting against the dissemination of records by those who collect them will prevent government agents from accessing them. See N.Y. GEN. BUS. LAW § 671 (McKinney 1996) (stating that the collection of video rental information poses "a serious threat to the personal privacy of New Yorkers"). Again, video surveillance undermines this assumption since it allows agents to acquire information about our public actions (or about items we carry in public) without asking for it.

personal interests. With ubiquitous video recorders, such a comprehensive picture might be pieced together from data gathered from outside the home as well.³⁰⁷

Not only would officials be able to watch and record acts of dissent or experimentation, facial recognition and modern databases allow them to immediately link these acts to a name and identity. We not only lose our privacy, but our anonymity. This loss would have consequences for freedom of expression and association, and the Supreme Court itself has noted this outside of the Fourth Amendment context. For example, in *NAACP v. Alabama*, the Court forbade the State of Alabama from compelling the NAACP to disclose its membership lists, and it stressed the “vital relationship between freedom to associate and privacy in one’s associations.”³⁰⁸ In *McIntyre v. Ohio Elections Commission*, it struck down an Ohio law prohibiting the distribution of anonymous campaign literature and took note of “a respected tradition of anonymity in the advocacy of political causes.”³⁰⁹ Most recently, in *Watchtower Bible and Tract Society of New York, Inc. v. Stratton*, the Court declared unconstitutional a town law requiring those who wish to canvass door-to-door to first identify themselves in a permit application filed with the mayor’s office and made available for public inspection.³¹⁰ In all of these cases, the government would not have needed to request information about the identities of group members, pamphleteers, or canvassers if it could simply review video records of their activities and match their images with faces and names in a biometric database. Just as it would be a strange result if technological “wizardry” enabling the government to see through walls could free it entirely from “the restraints mandated by the Fourth Amendment,”³¹¹ it would be odd if new

307. As Helen Nissenbaum notes, thanks to advances in computer technology, “information that was once scattered and transient may now be ordered, systematized, and made permanent” and computerized records are “public in a far more thoroughgoing sense than ever before.” Helen Nissenbaum, *Protecting Privacy in an Information Age: The Problem of Privacy in Public*, 17 LAW & PHIL. 559, 577–78 (1998). She argues that privacy of public information is needed to protect against routine aggregation of scattered details about someone and to guard against the release in one social context of information that is meant to be disclosed only in another. See *id.* at 581–90; see also RODNEY A. SMOLLA, *FREE SPEECH IN AN OPEN SOCIETY* 149 (1992) (noting that there not only will be “pressure on the law of torts” to make room for an “accumulation of public facts” tort, but also that it may one day be appropriate “to treat as a Fourth Amendment ‘search’ a law enforcement official’s decision to assemble before a single computer terminal all the information existing about a person in all the governmental data banks of all governmental agencies”).

308. 357 U.S. 449, 462 (1958).

309. 514 U.S. 334, 343 (1995) (citing *Talley v. California*, 362 U.S. 60 (1960)).

310. 536 U.S. 150, 166–69 (2002).

311. *United States v. Cusamano*, 83 F.3d 1247, 1265 (10th Cir. 1996) (finding, as the Supreme Court later did in *Kyllo*, that the government engages in a “search” under the Fourth Amendment when it uses infrared technology to “discover that which is shielded from the public by the walls of the home”).

visual surveillance and biometric technology allowed the government to simply take the information that the First Amendment forbids it from requiring people to provide.³¹²

Fourth, it is not merely the continuing observation of activities that undercuts privacy, but to an even greater degree, the ongoing recording of these activities. As Jeffrey Rosen notes, one of the distinctive features of modern America is the opportunity it gives individuals to “redefine and reinvent themselves every day” and “travel from place to place without showing their papers and being encumbered by their past.”³¹³ Such freedom cannot exist if individuals might at any time be confronted with a perfect record from a long-ago event. Indeed, the prospect of such a confrontation is likely to be unsettling even for those not interested in transforming their personae. Central to a free society is the individual’s sense that she will not have to justify her every action and expression to a government official. Making a record of activity for later review undermines this sense. It creates conditions making it far more likely that an individual will be challenged, years after the fact, with an event or statement that he might regret, or which—as a result of unpredictable developments in his own life or in the course of public events—places him in a new, deeply unflattering light. The creation of such a visual record of a person’s life is likely to cause anxiety not only because the government might view it, but because once a record exists, then rivals, acquaintances, friends, colleagues, or potential employers might one day view it too.³¹⁴ To the extent recording threatens to greatly expand the potential audience for every thing we say or do, notes Canadian Justice Gérard LaForest, it “annihilates the very important right to choose the range of our listeners [and watchers].”³¹⁵

For all of these reasons,³¹⁶ it seems appropriate for courts to rethink the common assumption that public officials do not invade privacy by

312. Other scholars have also stressed this caselaw on the First Amendment’s protection of anonymity and the extent to which large-scale public camera networks are in tension with it. See Nguyen, *supra* note 238, ¶ 48 (noting that courts have, in evaluating the constitutionality of face recognition, held “that there is no expectation of privacy in public places,” while they have “generally protected anonymity in *public spaces*” in cases such as *McIntyre*); Slobogin, *supra* note 38, at 257 (noting that camera surveillance “virtually nullifies” the efforts to maintain anonymity protected in *McIntyre* and similar cases).

313. Rosen, *supra* note 11, at 93.

314. This point was powerfully illustrated recently in England when local governments sold videotapes made from public surveillance cameras—for law enforcement purposes—to a sensationalist video maker who then screened embarrassing footage in a film called *Caught in the Act*. The film showed “sexual acts taking place in doorways, as well as harassments, muggings, car crimes, burglaries, and street fights” and showed “innocent victims, as well as the lawbreakers.” Burrows, *supra* note 179, at 1100.

315. *R. v. Duarte*, [1990] S.C.R. 30, 34.

316. And one might add one more reason, apart from the “informational privacy” concerns I have mentioned above, to provide safeguards against monitoring even in public—even when a

photographing or videotaping that which is visible to the public. But it is one thing to recognize that people need protection for privacy and anonymity in public places. It is another for courts to provide such protection. To do so, they have to overcome at least two significant hurdles, each of which underscores the difficulty of protecting privacy in areas open to view and helps demonstrate why it is so valuable to have clear boundaries provided by demarcated zones of privacy.

The first is that, without such clearly demarcated zones, it might become very difficult for courts to decide, and for individuals to predict, when a particular activity will receive Fourth Amendment protection. While some public activities, such as going to a doctor, may seem more personal than others, such as walking on a street with a friend, the importance of privacy in each situation will depend heavily on contextual details—What kind of a doctor's visit is it? Who is the friend one is walking with?—and will differ considerably from person to person. Some individuals may want to announce their political or religious beliefs to the world. Others may want to participate in politics or religion quietly, either because they simply view these beliefs as private business or because they wish to avoid creating tension with family members, friends, or acquaintances who do not share their views. Some activities, particularly biological functions, have been “traditionally shielded by great privacy.”³¹⁷ But much of what we want to keep from a large audience or an official audience is a matter of idiosyncratic preference. This underscores one advantage of a constitutional regime that provides people with recognized private spaces, like the home, and shielding devices, such as envelopes or containers, that they can use to shield whatever it is they happen to regard as private.³¹⁸ Unfortunately, such demarcated spaces and shielding devices are of limited value in protecting our public lives from intrusive observation, and, as I have noted above,³¹⁹ this is one reason that *Katz* itself did not fulfill its stated aspiration of extending constitutional privacy protection to public space.

person is not revealing any secrets, he may feel a sense of discomfort and confinement when being closely and steadily watched. Ruth Gavison points out that “concern for the opportunity to have solitude and anonymity is related not only to the wish to conceal some kinds of information, but also to needs such as relaxation, concentration, and freedom from inhibition.” Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 435 (1980).

317. See *Skinner v. Ry. Labor Executives' Ass'n*, 489 U.S. 602, 626 (1989) (commenting on the level of privacy afforded to the excretory functions).

318. See Heffernan, *supra* note 116, at 59 (noting that there are “‘idiosyncratic’ sources of vulnerability” that individuals protect through “resort to widely understood cues”—for example, a “closed door” or a “sealed envelope”—that signal their interest in withholding something from others).

319. See *supra* Part I.

There is also a second problem with expanding constitutional privacy protection to the public realm. Doing so could hamper law enforcement officials by tying their hands in the one space where they are free to vigorously pursue leads. Thus, the Court in *Olmstead* cautioned against reading the Fourth Amendment “search” constraints so broadly that courts “forbid hearing or sight.”³²⁰ Even after *Olmstead* was overruled by *Katz*, the Court again expressed the concern, in *Ciraolo*,³²¹ that preventing officers from freely viewing what is public would leave them with no place to start in investigating well-concealed criminal activity. Observation from a public place, the Court noted, is “precisely what a judicial officer needs to provide a basis for a warrant.”³²² One might argue that a society can afford to erect strong privacy protections around the home and other private places only because police can begin their investigation outside of such private areas and gather the evidence necessary to decide what intrusions into private areas are really essential.³²³ And constitutional restraint on police investigation could become even more crippling if police are locked into using primitive surveillance devices, while criminals or terrorists are left free to take advantage of emerging technologies to evade, or even surveil, the government officials trying to stop them. Placing constitutional constraints on the government’s observation of our public behavior might also seem pointless if the same activities we succeed in shielding from the police remain vulnerable to observation and videotaping by numerous private parties: if journalists and private investigators are allowed to point cameras at us in public, why can police not do so in order to more effectively thwart crime? While it is understandable that these two concerns may give courts pause in trying to establish privacy protections for public activities, neither of them presents an insurmountable barrier.

B. Securing an Architecture for Privacy (Not Just an Instance of It)

The concern that private activity in public spaces cannot easily be identified as such arises against the background of an unnecessary assumption: namely, that judges can apply the Fourth Amendment in public

320. *Olmstead v. United States*, 277 U.S. 438, 465 (1928).

321. *California v. Ciraolo*, 476 U.S. 207 (1986).

322. *Id.* at 213.

323. In *Kyllo*, Justice Scalia noted that one reason the court may have held that “visual observation is no ‘search’ at all” is to “preserve somewhat more intact our doctrine that warrantless searches are presumptively unconstitutional.” *Kyllo v. United States*, 533 U.S. 27, 32 (2001). If visual observation constituted a search, then in order to avoid requiring police to request a warrant for every visual examination, the Court would have to expand the category of *reasonable* “warrantless searches.”

spaces only by making a case-by-case judgment of whether specific activities or objects are constitutionally shielded. It is such judgments that raise difficulties, because judges are ill-equipped to distinguish between “protected private activities” and “unprotected public activities” where different individuals might make different and inconsistent decisions about what specific activities deserve to be shielded. To be sure, the Supreme Court has hinted that in certain cases, it might draw such distinctions to protect certain details from being photographed or observed, even in public, with high-powered cameras or telescopes. In *Dow Chemical*, it noted that Fourth Amendment concerns might arise if the government used satellites to reveal “intimate details” such as a “class ring” or “secret documents” or any “identifiable human faces.”³²⁴ But it is difficult to see how courts can authoritatively identify what kinds of details count as “intimate details.”³²⁵ In any event, it may be important for many people to keep private even some details about their lives that it would be unusual to characterize as “intimate.”³²⁶

The more promising approach is to recognize that judges need not make any such distinction between different private activities. They do not need to designate certain activities as insulated from surveillance and others as available for whoever wishes to observe or record them. Rather, just as the device of “constitutionally protected zones” in twentieth-century Fourth Amendment jurisprudence gave individuals the power to decide for themselves what to shield in a home, office, or a suitcase, so twenty-first century Fourth Amendment jurisprudence should similarly recognize that the object of Fourth Amendment protections in public space is not to micromanage individuals’ attempts to preserve privacy in the public sphere,

324. *Dow Chem. Co. v. United States*, 476 U.S. 227, 238–39 n.5 (1986).

325. See *Kyllo*, 533 U.S. at 238–39 (noting the difficulty of developing a “jurisprudence specifying which home activities are ‘intimate’ and which are not” and the difficulties that police officers would have applying such a jurisprudence even if it were developed); see also Christopher Slobogin, *Technologically-Assisted Physical Surveillance: The American Bar Association’s Tentative Draft Standards*, 10 HARV. J.L. & TECH. 383, 399 (1997) (noting that factors focusing on the nature of activity or object are “of questionable relevance to the extent it forces distinctions between ‘intimate’ and ‘non-intimate’ objects—into which category does one place clothing, book covers, or unoccupied living rooms?”).

326. For example, while someone’s possession of a law text or an accounting book hardly seems to be an “intimate detail,” it may well reveal something that person prefers to keep from certain audiences, for example, an interest in a new career at odds with the wishes of family members or current employers. Moreover, as Dorothy Glancy notes in discussing fears about Intelligent Transportation Systems, it is not reassuring to people that “ITS information is not very personal or private, when compared, for example, with data about a person’s health or financial status. People seem to be concerned when a comprehensive information profile is constructed about any aspect of their lives.” Dorothy J. Glancy, *Privacy and Intelligent Transportation Technology*, 11 SANTA CLARA COMPUTER & HIGH TECH. L.J. 151, 165 (1995).

but rather to guarantee that the public sphere retains a character that continues to provide individuals the opportunities to preserve privacy where they believe they need it. In other words, courts might recognize and legally secure the privacy-protecting features of those environments rather than simply protecting the privacy of a particular activity within them.³²⁷

This still leaves the question of how courts are to go about identifying and protecting those features of our public environment that provide essential support for privacy and anonymity. One means of protecting the privacy-protecting features of our public environment is to subject the government to some of the same social norms that we expect other individuals to follow. According to William Heffernan, this emphasis on social norms is already at the heart of Harlan's "reasonable expectations test," because one cannot tell what expectations "society is prepared to recognize as 'reasonable'" unless one looks at "society's practices," and specifically at "privacy norms."³²⁸ Even if the Court were to abandon the "reasonable expectations" test, it could not easily ignore social norms in protecting Fourth Amendment privacy interests, because they are a central and indispensable condition for the privacy individuals enjoy in modern society. Even when individuals are able to hide their activities behind a physical barrier, they often rely on social norms to ensure that these activities stay hidden. There are powerful norms, for example, against opening sealed letters or peering through cracks in closed doors. Such norms, of course, provide protection of information in houses or enclosed spaces. But they also operate in public streets and parks. For example, even in such open environments, as Jeffrey Rosen points out, it is rude to stare at someone.³²⁹ Although it is hard to conceive of norms that might shield individuals in such public environments from all observation whatsoever (at least not without making such environments considerably less free), existing norms do shield individuals from sustained, unconsented-to attention.

As Heffernan shows, attention to social norms provides a way to critique some recent, puzzling Fourth Amendment cases, in which the Supreme Court has allowed government to engage in behavior usually deemed at odds with social norms.³³⁰ Thus, while people might be horrified

327. As Justice Scalia made clear in *Kyllo*, this is what the Court has done with respect to the interior of the home: "there is no exception to the warrant requirement for the officer who barely cracks open the front door and sees nothing but the nonintimate rug on the vestibule floor. In the home . . . all details are intimate details, because the entire area is held safe from prying government eyes." *Kyllo*, 533 U.S. at 37.

328. See Heffernan, *supra* note 116, at 36–37.

329. JEFFREY ROSEN, *THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA* 16 (2000).

330. Heffernan, *supra* note 116, at 80–126.

and complain if their neighbors rummaged through their garbage bags, the Fourth Amendment, as interpreted by the Supreme Court, does not stop or hinder police from doing so.³³¹ While people would probably believe they had been subjected to a substantial injustice if another person feigned friendship in order to spy upon them or gain access to personal confidences, the Fourth Amendment does not stop a government informer from feigning friendship to learn more about the target of an investigation.³³² As Heffernan argues, courts should rethink granting police unfettered discretion to exploit and violate well-established norms, and more consistent adherence to privacy norms might provide some protection against untrammelled video surveillance of streets and other public spaces.³³³ One might argue that video surveillance functions as a norm-circumventing device in that it allows police to observe people from a distance in ways that would be considered impolite and unacceptable on the scene. As Jennifer Granholm notes, a “cop on his beat” may be unlikely to stare at an innocent person in a way that flouts “norms or human decency” when he is “observed by others whose observation forces a certain civility and a modicum of rationality.”³³⁴ By contrast, a hidden watcher at a monitor is “unchecked” by norms of social interaction.³³⁵

But while widely-accepted norms of privacy help us analyze the application of the Fourth Amendment to government informers or government snooping into our possessions, they are less useful for analyzing when video surveillance and other new technologies are acceptable in battling crime and terrorism. This is because it is existing norms themselves, and not just judicial misinterpretation of those norms, which often give the government privileged access to some of our information in the name of security. For example, it seems likely that many people entering airports do

331. *See California v. Greenwood*, 486 U.S. 35, 37–43 (1988) (finding that police did not violate the Fourth Amendment when, without a warrant, they seized and rummaged through a sealed garbage bag left on the curb); *see also* Heffernan, *supra* note 116, at 92 (noting that “people usually signal an interest in privacy for their garbage” by “wrap[ping] it in opaque bags tied at the top” and that, by allowing police to rummage through it anyway without probable cause, the Court ignored this norm and instead used the behavior of norm-violators, or “snoops,” as a baseline for what is reasonable).

332. *See* Heffernan, *supra* note 116, at 106, 109 (noting that, under existing privacy norms, “outsiders who use deceit or who try to induce betrayal in order to penetrate intimate relationships can properly be charged with invading insiders’ privacy” and describing the Court’s refusal to protect this norm as “the most profound error in the Court’s jurisprudence of undercover operations”).

333. *See id.* at 126 (arguing that the Court’s Fourth Amendment jurisprudence should “capture[] the privacy norms of everyday life” and that this would “place[] modest, but wholly justified, limits on law enforcement activities”).

334. Jennifer Mulhern Granholm, *Video Surveillance on Public Streets: The Constitutionality of Invisible Citizen Searches*, 64 U. DET. L. REV. 687, 698 (1987).

335. *Id.*

not view it as a violation of social norms for a government official to search their bags. Indeed, the airport scenario is in a sense the inverse of the informer situation. In the case of a secret informer, we reveal information to a friend that we would presumably not reveal to an official who is a stranger to us, and are horrified when a “friend” turns out to be an agent merely playing that role. By contrast, in airports, we submit to systematic examinations from security personnel that we would not necessarily tolerate from private acquaintances or even friends, and we might well be upset if the person in a uniform rummaging through our suitcase was not an official at all, but an acquaintance in disguise trying to learn more about our lives.³³⁶ Governments undertaking overt video surveillance in a street or subway might well argue that this surveillance bears a much closer resemblance to the airport security measure than it does to uninvited staring by a passerby on a street corner.

In the context of analyzing video surveillance and other forms of technologically-assisted surveillance of public places, it therefore makes sense to focus more closely on another source of privacy protections. Social norms are not the only source of opportunities for privacy and anonymity in public spaces. Rather, they are only one component of a larger social and physical environment whose structure makes privacy and anonymity—and with it, a good deal of modern individual liberty—possible. One key feature of this environment, apart from social norms, is what one might refer to as “the architecture of public space.” As Lawrence Lessig explains in his discussion of Internet architecture, different possible constructions of the space in which we move and act, whether it is virtual or physical space, can have radically different consequences for free speech, privacy, and other core constitutional values. As Lessig notes, “[s]paces have values. They express these values through the practices or lives that they enable or disable. Differently constituted spaces enable and disable differently.”³³⁷ Lessig and other privacy law scholars, such as Joel Reidenberg³³⁸ and Daniel Solove,³³⁹

336. In fact, one commentator argues that because the *Katz* reasonable expectations test is “dynamic rather than static” and because, however objectionable it may have been in the past, airport security screening is now “routine,” “it is highly questionable whether one truly holds a reasonable expectation of privacy in either their person or effects” at an airport gate. John Rogers, Note, *Bombs, Borders, and Boarding: Combatting International Terrorism at United States Airports and the Fourth Amendment*, 20 SUFFOLK TRANSNAT’L L. REV. 501, 543 (1997). For reasons explained below, *infra* Part IV, such an approach confuses the “search” and “reasonableness” inquiries by holding that when it is reasonable for people to expect government intrusion into a private area (for example, to serve a crucial safety interest), the “privateness” of the area necessarily fades.

337. LESSIG, *supra* note 101, at 64.

338. See Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEXAS L. REV. 553, 554–55 (1998) (arguing that “system design choices impose rules on participants” and that this is important for policymakers to understand).

have already stressed the importance that architecture often has for privacy and should have in privacy law. As Solove notes, “physical architecture can determine what is visible or hidden,” and by shaping the physical and social environment in which we move, “[l]aw . . . shapes our ability to hide information and it influences information accessibility.”³⁴⁰

The role that architecture plays in enabling privacy and anonymity is often less noticed than that of social norms for two reasons. First, while people can imagine violating prevalent norms, as people sometimes do, and while they may well know of communities with different norms—for example, social or religious groups where members expect to know about other members’ day-to-day lives—they are less likely to imagine a world where the spatial environment operates in very different ways. Even in communities that do not share our norms, walls and other barriers still block others from viewing private activities, and great distances generally make observation more difficult. It is only in science fiction worlds like that described by Lewis Padgett, where walls record activities instead of concealing them,³⁴¹ that we typically receive a clear picture of how the environment may operate differently.

Second, perhaps because of its seemingly natural and permanent quality, the larger environment is seen not as a possible instrument of a privacy violation, but as an unalterable backdrop against which such a violation occurs. This way of thinking about Fourth Amendment privacy is also likely to follow from a literalist interpretation of the word “search” in the Fourth Amendment’s text: officials conduct a search by foraging through existing hiding spaces in order to find a person or to locate information. By contrast, it is somewhat odd to describe them as “searching” when, as a matter of public policy, they decide to clear society (or some portion of it) of

339. See Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 HASTINGS L.J. 1227, 1240–41 (2003) (“Our environment is not only shaped spatially by the architecture of buildings and the layout of cities, but by the design of information systems.”).

340. *Id.* at 1240–41. Solove’s conception of privacy’s “architecture,” however, is somewhat different from Lessig’s. For Lessig, norms and laws represent one kind of constraint, while architecture—the structure of the environment in which we move—represents another. See LESSIG, *supra* note 101, at 86–90 (explaining the effects of four constraints—law, norms, markets, and architecture—on the objects that are regulated by those constraints). The boundary lines between these types of constraint are not firm, but they serve an important analytical purpose. By contrast, Solove appears to use “architecture” to mean all “legal and social structures,” including constitutions, laws, and norms. See Solove, *supra* note 339, at 1239; see also Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1087 & n.19 (2002) (explaining that Solove uses the term “architecture” more broadly than Lessig does). In this Article, I will follow Lessig’s usage in order to stress the contrast between the approach defended here and other approaches (like David Brin’s), which put more emphasis on norms in responding to emerging surveillance systems. See *infra* Part V.

341. See *supra* Introduction.

the havens where people might seek refuge from observation. If they do the latter, one might argue, officials are not “searching,” but rather sparing themselves the need to search in the future. If desired information (or video archives) can be instantaneously spotted or called up by the government at any moment, there will be no need for anybody to look for it. Rather, thanks to new kinds of visual surveillance, it will be as much in plain view as something that is right before a police officer’s eyes.

The problem with such a literalist approach to the meaning of a Fourth Amendment “search” is that it leaves information-hungry officials the option of carving a path around important constitutional hurdles: where the Fourth Amendment bars searches, they can respond by making it harder to escape their gaze. Such an approach hardly secures the interests that the Fourth Amendment is meant to protect. As Edward Shils has noted, “[t]he separateness of places” and “the impenetrability of their physical boundaries” have been two of “the main bulwarks of that privacy which human beings have possessed or desired to possess through most of history” and that “[c]hanges in . . . these affect the magnitude of the privacy that a society enjoys.”³⁴²

The privacy-protecting features of homes and offices are quite familiar. People block observation and aural monitoring with walls and window curtains. But as is true with norms protecting us from observation, spatial features help thwart observation not only in environments recognized as private, like the home, but also in streets and public squares. The architectural features of public space that protect privacy and anonymity are not as tangible as walls and barriers, but they are no less important. Our freedom to act spontaneously, or to inform ourselves about new and controversial beliefs, depends in large measure on the fact that our world operates in such a way that these acts generally leave no record, unless we take the time and care to produce one. As Solove has noted, many “small details” about our lives are captured only in “dim memories or fading scraps of paper.”³⁴³ Today, some of these details are “preserved forever in the digital minds of computers,”³⁴⁴ but for the moment, we are not in a world where this is generally true of the activities or communications in which we engage in public spaces. Likewise, the anonymity and relative privacy we expect in public life is possible only because our world is built in such a way that, to the extent our action does leave traces, in people’s memories or records, of what we have done, these visual records of our daily lives are not naturally

342. Edward Shils, *Privacy: Its Constitution and Vicissitudes*, 31 LAW & CONTEMP. PROBS. 282, 288 (1966).

343. See Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1391, 1394 (2001).

344. *Id.*

gathered together in any centralized database accessible to others. We rely also, in our public lives, on the possibility of merging into a crowd or becoming an unrecognized part of people's "situational landscape."³⁴⁵ We rely on possibilities for finding seclusion in public space, or for reading a letter or carrying on a conversation with substantial confidence that no one, not even a snoop or other violator of social norms, is close enough to see or hear.

It is not only the physical environment that individuals have relied upon to provide a stable background for privacy in public places, but also the social structure of the world they move in. By this I mean not specific norms or social rules, which people can violate, or imagine violating, but rather certain features of the social environment that often shape individuals' interactions with each other in more subtle and irresistible ways. For example, the fragmented nature of modern social life makes it likely that individuals will interact with different groups of people in the different spheres of life—in their home and family lives, their workplaces, their religious lives, their political lives, or their interactions with government officials—and this makes it much more difficult than it otherwise would be for our associates to gain a thorough familiarity with all of our interests, beliefs, and plans. While we usually take for granted all of these features of the public environment, physical and social, technological developments now occurring in video and tracking technology not only make a radical change in the architecture of public space conceivable, they make it likely.³⁴⁶

This focus on the architecture of privacy in public space might seem alien to existing Fourth Amendment jurisprudence. Few court opinions have expressly spoken in terms of protecting an environment or "architecture" for privacy in public life. Moreover, it seems implausible to suggest that the Fourth Amendment's language on searches and seizures should give the judiciary a veto on *all* state action that significantly impacts the structure of our physical and social environment.

In fact, one might argue that to the extent preservation of Americans' privacy depends on managing our environment rather than shielding specific individuals' activities, it is a task for legislators and administrators rather than for judges. Administrators and legislators, as Donald Horowitz points out, have both a broader mission and "a wider range of tools in their kit" than judges empowered to resolve particular disputes with specified remedies: they are better-equipped to engage in extensive fact-finding, to stay abreast

345. See Gutterman, *supra* note 118, at 706. ("In these public acts we do not expect to be personally identified and subject to extensive surveillance, but seek to merge into the 'situational landscape.'").

346. See BRIN, *supra* note 16, at 9 (describing the capacity of cameras to transform our large complex society into a "vast but easily spanned village").

of technological developments, and to pass (and experiment with) broad and complex regimes of privacy protection.³⁴⁷ And there is another reason that one might give for preferring a statutory rather than a constitutional solution to the dangers of video surveillance: if democratic majorities are willing to part with some of their privacy to increase their safety (or perceived safety), then why should judges be constitutionally empowered to veto this choice? The Bill of Rights protects minority rights from oppressive majorities, but such a measure seems ill-fitting when a democratic society is turning cameras not only on minorities, but on all of its citizens. Perhaps it is with such considerations in mind that the majority in *Katz* emphasized that “the Fourth Amendment cannot be translated into a general constitutional ‘right to privacy’” and that while it “protects individual privacy against certain kinds of governmental intrusion, . . . its protections go further, and often have nothing to do with privacy at all.”³⁴⁸

Such arguments provide good reason for courts to avoid imitating administrators and wrenching away the choices that rightfully belong to democratic majorities (including the right to make foolish, but constitutionally permissible choices). They do not, however, provide good reason for courts to ignore the physical and social architecture of privacy in their Fourth Amendment caselaw. First, as noted earlier, where a government-imposed transformation of our surroundings serves as the functional equivalent of a search—where, for example, it makes transparent to observation barriers that it is constitutionally barred from crossing—then it seems puzzling to say that one can only rely on a statute (or regulation) to guard against such an end run around the Constitution. Second, while majorities have the right to adopt unwise surveillance regulations, they do not have carte blanche power under the Constitution to adopt or approve arrangements that reduce liberty or privacy below constitutional minimums: Just as they are barred from adopting even content-neutral speech restrictions where such restrictions leave citizens with too little liberty of expression, and would be barred from passing laws that make all homes (including their own) subject to warrantless searches, so they may be barred from adopting designs that leave citizens subject to instant identification and limitless surveillance in public spaces.

Courts are also not helpless to protect the environmental conditions that sustain privacy. They are admittedly ill-equipped to exercise power or oversight over the detailed architecture of public space: they cannot design roadways, law enforcement methods, or communication systems. But they are not powerless to judge when the surveillance schemes involved in a particular dispute leave citizens with too little privacy. Indeed, an

347. DONALD L. HOROWITZ, *THE COURTS AND SOCIAL POLICY* 35 (1977).

348. *Katz v. United States*, 389 U.S. 347, 350 (1967).

“architecture-based” approach to the Fourth Amendment has a close kinship with a judicially-based alternative to the *Katz* “private expectations” test.

This alternative to *Katz* was formulated by the same person who formulated the *Katz* test itself. In his dissenting opinion in *United States v. White*, Justice Harlan cast doubt upon the expectations test he had offered only a few years earlier.³⁴⁹ Judges applying the Fourth Amendment, Justice Harlan said, should not “merely recite the expectations and risks without examining the desirability of saddling them upon society.”³⁵⁰ They should examine instead “the nature of a particular practice and the likely extent of its impact on the individual’s sense of security.”³⁵¹ To be sure, Justice Harlan noted that whatever privacy concerns might arise should be “balanced against the utility of the conduct as a technique of law enforcement,” and this side of the balance, as explained below, is now provided by the Court’s “reasonableness” inquiry.³⁵² However, the language of his dissent suggested that such balancing of privacy and safety concerns was to come only after a court first decided whether Fourth Amendment privacy interests were threatened in any way. In defining what constitutes a “search” of the sort subject to Fourth Amendment protection, the key concern was whether the surveillance technique in question would “jeopardize the sense of security [against monitoring] which is the paramount concern of Fourth Amendment liberties.”³⁵³ When a technique does significantly jeopardize “this sense of security”—when it leaves us vulnerable to random detention or monitoring by government officials—Justice Harlan seemed to suggest that, regardless of the safety benefits it might hold, Fourth Amendment limits would be necessary because “more than self-restraint by law enforcement officials [would be] required” to make its use safe for core individual privacy interests.³⁵⁴

Other commentators have proposed a similar test. In a widely-cited article discussing the *Katz* test, Anthony Amsterdam proposed that in answering the question of what is a “search,” courts must make “a value judgment . . . whether, if the particular form of surveillance practiced by the police is permitted to go unregulated by constitutional restraints, the amount of privacy and freedom remaining to citizens would be diminished to a compass inconsistent with the aims of a free and open society.”³⁵⁵ Rather than focus solely on whether an individual had a right to expect privacy in a given instance, and in a given activity, Justice Harlan and Amsterdam appear

349. *United States v. White*, 401 U.S. 745, 768 (1971) (Harlan, J., dissenting).

350. *Id.* at 786.

351. *Id.*

352. *Id.*; see also *infra* Part VI.

353. *White*, 401 U.S. at 786 (Harlan, J., dissenting).

354. *Id.*

355. Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 403 (1974).

to invite courts to place the focus where it should be: on the consequences that a type of surveillance or investigation has on the social and physical environment which makes privacy and anonymity, and with them, individual autonomy, possible in the first place. Such an approach would protect people against public video surveillance not only when such surveillance is aimed at a “private activity or condition,” as the current ABA Standards on video surveillance require,³⁵⁶ but whenever surveillance is unconstrained by firm limits preventing harm to the privacy- and anonymity-enabling features of public space. And because this approach focuses courts’ attention on forms of surveillance, it does not transform the Fourth Amendment into a license for judges to review and constrain all government measures that might have some impact on citizens’ privacy.³⁵⁷

One might worry that by extending privacy protection in this way, courts would weaken its force. As David Sklansky notes, the “failure to distinguish between the home and areas outside the home has resulted in diminished privacy protection for the home To say that [the Fourth Amendment] applies everywhere equally is to say that it protects nowhere very strictly.”³⁵⁸ One might offer similar reasons for continuing to focus privacy-protection on “intimate” activities. As difficult as it is to draw a clear boundary line between “intimate” and “nonintimate” activities,³⁵⁹ the argument goes, privacy protection in modern life simply cannot do without such a distinction. In an age when the modern administrative state routinely demands, and receives, substantial information about citizens’ financial condition, work life, and education, it might seem crucial for courts to

356. ABA STANDARDS OF CRIMINAL JUSTICE, *supra* note 147, Standard 2-9.3, at 15–16. The definitions section of the Standards expressly ties the determination of whether an activity or condition is private to the reasonable expectations test: “An activity, condition, or location is private when the area where it occurs or exists and other relevant considerations afford it a constitutionally protected reasonable expectation of privacy.” *Id.* at Standard 2-9.2, at 15. Because the reasonable expectations test can be reinterpreted to take account of the privacy-protecting features of public space, one might be able to effectively protect individuals’ privacy in public life by retaining the ABA’s definition, but adopting a revised position on what conditions make it reasonable to expect protection against government monitoring.

357. This exclusive focus on surveillance might seem problematic. Even where government does not intend to gather information about its citizens, it might unwittingly make them far more vulnerable to future monitoring (e.g., by mandating that cell phones come with technology allowing quick location of 911 callers). Admittedly, such a program could weaken the privacy the Fourth Amendment is meant to protect, but it is hard to characterize it as a search or its functional equivalent. And extending “search and seizure” protections to such measures would make it hard to put meaningful limits on the scope of the Fourth Amendment, since every statutory or administrative regulation that affects citizens’ physical or informational environment could conceivably be characterized as affecting citizens’ privacy.

358. Sklansky, *supra* note 102, at 193–94.

359. *See, e.g.,* *Kyllo v. United States*, 533 U.S. 27, 38 (2001) (claiming that “it would be impractical in application” to prohibit thermal imaging of intimate details while allowing imaging of non-intimate ones).

distinguish such “nonintimate” information, which the state has a right to ask about, from “intimate” details of personal, family, and religious life, which the state presumably does not.³⁶⁰ Otherwise, we will be as vulnerable to the state as autonomous individuals and family members as we are when we are in our “public” roles as students, workers, citizens, or taxpayers.

At most, however, such arguments provide reasons why courts, or perhaps more appropriately, legislatures, might provide additional protection, above and beyond the general freedom from unreasonable monitoring provided by the Fourth Amendment, for certain spheres we define as “intimate.” Courts have certainly provided such protection by “decisional privacy” cases such as *Roe v. Wade*³⁶¹ and *Griswold v. Connecticut*,³⁶² and they have arguably done so in holding, in the case of *Whalen v. Roe*, that the Fourteenth Amendment includes a right of informational privacy in matters which are “personal in character and potentially embarrassing or harmful if disclosed.”³⁶³

As an interpretation of the Fourth Amendment, the above arguments are both too limited and too pessimistic. They are too limited because by protecting only certain limited or in-home activities, they fail to offer sufficient protection against comprehensive observation of the sort made possible by devices like Lewis Padgett’s “past-tracing” or George Orwell’s “telescreens.” What is suffocating about a world defined by unconstrained use of such devices is not simply that the state might pick up “intimate” along with “nonintimate” activities, or that its gaze may stray into the home or other private places. It is that a state observer is in some sense always with us, giving rise to a self-consciousness about every action and probably, for many people, a fear that state actors, or private parties cooperating with them, will one day seek to hurt us with records of these activities, even those we currently regard as “nonintimate” and “nonprivate.” To protect against such corrosion of freedom in public life, it is therefore insufficient to draw a

360. One might make such an argument in part to answer the challenge posed by William J. Stuntz to the very idea that privacy ought to remain the principal focus of the Fourth Amendment. Stuntz argues that strong constitutional privacy protections are in tension with many aspects of the administrative state and puzzlingly give “criminal suspects *more* privacy protection than ordinary citizens get from government employers, tax collection agencies, and the like.” William J. Stuntz, *Privacy’s Problem and the Law of Criminal Procedure*, 93 MICH. L. REV. 1016, 1046 (1995).

361. 410 U.S. 113, 152–53 (1973) (recognizing a constitutional right of privacy in decisions regarding marriage, procreation, contraception, family relationships, and child rearing) (citations omitted).

362. 381 U.S. 479, 485 (1965) (striking down a law restricting the use of contraceptives because it interfered with the marital privacy right protected under the Fourth Amendment); *see also* *Eisenstadt v. Baird*, 405 U.S. 438, 453 (1972) (noting that if the right of privacy means anything, it means “to be free from unwarranted governmental intrusion into matters so fundamentally affecting a person as the decision whether to bear or beget a child”).

363. 429 U.S. 589, 605 (1977).

circle of protection only around certain activities; courts, as Justice Harlan and Amsterdam appeared to recognize, have to guard against all kinds of surveillance that have broad effects on the nature of our public spaces.³⁶⁴ Indeed, any approach that did less would hardly provide a realistic constraint on public video surveillance. Since cameras cannot easily be programmed to ignore intimate acts or details, human operators could likely apply an “intimate facts” standard only by having someone view *all* of the images that a camera captures in order to make judgments about which are intimate and which are not.

Arguments which limit constitutional privacy-protection to intimate activities are also too pessimistic in thinking that by stretching constitutional privacy protection to cover public life, judges will weaken it everywhere, particularly in the home. The Fourth Amendment jurisprudence defended here does not require that courts treat the home as equivalent to public space for Fourth Amendment purposes. It requires that courts preserve the privacy-protecting features distinctive to each of these environments. In the home, of course, walls and windows, in combination with property rules and social norms, allow us to exclude the rest of the world far more easily and completely than we are able to anywhere in public space, and courts might well acknowledge this in adopting “bright line” protections against searches in the home that they cannot apply elsewhere. Courts, however, might still vigorously protect privacy in public space, but do so in a different manner. For example, they might allow police observation in public places that would be unacceptable if directed through the windows of a home, but still limit the use of surveillance techniques, like biometrically-equipped camera networks, which can quickly destroy the anonymity people find in crowds or the seclusion they find in isolated portions of a park or public library. Such protection of public space would almost certainly rule out unconstrained video surveillance of public space, but it is possible to conceive of certain more limited uses of video surveillance that would leave the core privacy-protecting features of our public environment intact, or alternatively, to build functionally-equivalent privacy protections into a new technological landscape.³⁶⁵

364. See *United States v. White*, 401 U.S. 745, 787 (1971) (“Were third-party bugging a prevalent practice, it might well smother that spontaneity—reflected in frivolous, impetuous, sacrilegious, and defiant discourse—that liberates daily life.”); Amsterdam, *supra* note 355, at 377 (noting that “any number of categories, however shaped, is too few to encompass life and too many to organize it manageably”).

365. This Article will explore these possibilities in greater depth. See *infra* Parts IV–V.

C. Reconciling Fourth Amendment Freedom with Technological Progress and Effective Policework

As noted earlier, the desire for clarity is not the only reason that courts have protected Fourth Amendment privacy rights most vigorously in the home and other traditionally-private settings, while leaving observation of public activities largely outside the reach of the Fourth Amendment. Courts have also worried that classifying public space as a "private zone" will leave police with no space to vigorously pursue leads. If all close scrutiny in public becomes a "search," law enforcement officers might well find themselves in a kind of Catch-22, wherein they cannot conduct a search until they show probable cause, but cannot uncover evidence providing probable cause without first engaging in a search. Thus, as the Supreme Court stressed in *Ciraolo*, police must be given some way to gather evidence of probable cause without violating the Constitution.³⁶⁶

One way to answer to this challenge is to point out that law enforcement has been able to find probable cause for searches even without extensive video surveillance. In *United States v. Biasucci*, the government requested a warrant to install video cameras only after receiving information from confidential sources and using undercover agents.³⁶⁷ Even in cases when courts allowed police to use public video surveillance without a warrant, the police generally did so not as a first step in detecting criminal activity, but only after receiving a tip that led police to suspect that criminal activity may be occurring in a particular location.³⁶⁸ Even with Fourth Amendment limits on video surveillance, law enforcement would still have space to gather evidence of criminal activity.

Such an answer is not wholly satisfactory. That police have been able to fight crime without a particular technology in the past does not mean they should be constitutionally barred from using that technology in the future. New threats, such as emerging forms of terrorism, may require new techniques to combat them. Thus, when plane hijacking emerged as a security threat in the late 1960s and 1970s, courts did not require the government to rely solely on tips or other traditional methods of police work; they allowed screeners to use metal detectors, even in the absence of

366. See *California v. Ciraolo*, 476 U.S. 207, 213 (1986) (noting that observation from a public vantage point is "precisely what a judicial officer needs to provide a basis for a warrant").

367. 786 F.2d 504, 511 (2d Cir. 1986).

368. See, e.g., *Rodriguez v. United States*, 878 F. Supp. 20, 22 (S.D.N.Y. 1995) (allowing the recording of the front of an apartment building after an undercover agent provided a tip that the sale of illegal narcotics would occur there); *State v. Holden*, 964 P.2d 318, 319 (Utah Ct. App. 1998) (allowing the videotaping of the defendant's front yard after his neighbor reported an unusual volume of suspicious visitors).

probable cause.³⁶⁹ Even when police are focusing on more familiar crimes, such as armed robbery or rape, people understandably and justifiably want the government to take advantage of new technologies to solve and prevent these crimes.

Moreover, there is another ground one might give for viewing the Fourth Amendment jurisprudence proposed here as dangerously Luddite in character: it attempts to immunize certain aspects of the physical and social environment against what some see as inevitable change. According to David Brin, for example, video cameras are proliferating rapidly and “the *djinn* cannot be crammed back into its bottle.”³⁷⁰ No matter how many laws are passed, “it will prove quite impossible to legislate away the new surveillance tools and databases,” and we must therefore reconcile ourselves to a world where “[l]ight is going to shine into nearly every corner of our lives.”³⁷¹ And any judicial effort to protect people from this harsh light is made considerably more difficult by the fact that such light is shining into people’s lives not only from government-controlled networks of cameras, but from a multitude of different sources, including curious neighbors, journalists, and private companies. Miniature cameras and sophisticated satellite tracking equipment are heavily advertised and easily acquired on the World Wide Web, and cell phones with built-in cameras are increasingly affordable and widespread.

Rather than try pointlessly to turn back the march of technology, says Brin, free societies should focus on saving what can still be preserved in a world of ubiquitous cameras, namely, such societies’ commitment to freedom and equality.³⁷² Instead of trying to eliminate the power of comprehensive surveillance (a futile task), democratic societies should ensure that this power is exercised democratically and made available to all, by giving all citizens access to the camera systems, allowing them not only to watch each other, but to watch over the way the police and other public officials do their jobs.³⁷³ Privacy will still exist, Brin believes, but not as an unsustainable legal graft by courts onto a social and technological environment that cannot sustain it. Rather, it will exist in the form of social

369. See, e.g., *United States v. Epperson*, 454 F.2d 769, 771 (4th Cir. 1972) (“The danger [incident to air piracies] is so well known, the governmental interest so overwhelming, and the invasion of privacy so minimal, that the warrant requirement is excused by exigent national circumstances.”); *United States v. Slocum*, 464 F.2d 1180, 1182 (3d Cir. 1972) (“[W]e conclude that within the context of a potential hijacking the necessarily limited ‘search’ accomplished by use of the magnetometer *per se* is justified by a reasonable governmental interest in protecting national air commerce.”).

370. BRIN, *supra* note 16, at 8.

371. *Id.* at 9.

372. *Id.* at 23.

373. *Id.* at 23–24.

norms that people voluntarily adopt and adhere to. Because those who invade others' privacy with ubiquitous video surveillance can be watched even as they do so, they will be subject to potentially intense pressure by peers, and perhaps associations of interested citizens, to use surveillance only in socially appropriate ways.³⁷⁴

Arguments such as Brin's provide an invaluable reminder that the physical and social foundations of constitutional liberalism can shift dramatically, forcing those who support individual rights to think carefully about how such rights can continue to flourish in new and unfamiliar conditions. However, this argument does not take adequate account of the role that privacy law, and Fourth Amendment jurisprudence in particular, can play in adapting long-standing liberties to evolving social and technological environments. Instead, Brin seems to place great confidence in the power of social norms alone to tame the threat that expansive video surveillance presents to individual liberty. Yet a state with a strong interest in acquiring information might not be any more deterred by existing privacy norms than it is by existing norms against rummaging through garbage or the use of false friends.³⁷⁵

Apart from overestimating the power of privacy norms to stave off pervasive monitoring, this argument also underestimates the role that law can play in shaping emerging technologies. Brin sometimes seems to view law as condemned simply to react to changes in the social and technological landscape: certain technologies alter the world we live in, and courts must then adapt themselves to this world.³⁷⁶ But rather than simply act as passive

374. Brin's proposal is not unlike the public video surveillance system put into effect in Anchorage, Alaska, in which "video images from street surveillance cameras are not transferred to a police department; instead, they are sent to private residents' home computers." Burrows, *supra* note 179, at 1103. Cincinnati residents have experimented with a similar scheme. Liza Porteus, *Cincinnati Residents Try High-Tech Crime Stopping*, FOX NEWS.COM (July 15, 2003) (describing the efforts of Cincinnati citizens to reduce street crime by monitoring a system of networked cameras), at <http://www.foxnews.com/story/0,2933,91885,00.html>.

375. See *supra* subpart III(B). There are also other difficulties with relying solely on social norms to safeguard privacy. First, there is a practical difficulty to enforcing such norms: if people do not know *who* is likely to be watching them, they will not easily be able to observe those observing them. It is possible, perhaps, to imagine some technology that alerts each person to her audience at any given moment. But even if such technology allowed some privacy norms to survive in a society where people found themselves under the constant glare of cameras, it is not clear that those with dissenting views or others wishing to engage in unconventional behavior would benefit from the norms embraced by the majority. As Lawrence Lessig points out, "[w]hen we live in multiple communities, accountability becomes a way for one community to impose its view of propriety on another." LESSIG, *supra* note 101, at 153.

376. See BRIN, *supra* note 16, at 12–14 (arguing that increased legal protection of privacy can diminish privacy by encouraging the development of more discreet and intrusive technologies). Brin does not unequivocally reject the use of legal controls to counterbalance governmental monitoring. On the contrary, in one part of his case for a transparent society, Brin says that

witnesses to major technological changes, courts can and should play a role in determining how such developments unfold.

More specifically, when the architecture of privacy begins to break down under pressure from new surveillance technologies, courts can do two things to restore their privacy-protecting functions. First, when architectural barriers cease to keep out prying government eyes, laws might do so instead.³⁷⁷ As Lawrence Lessig has observed, architectures, norms, and laws (and, he adds, market forces) all function as constraints on behavior, and one sort of constraint can often be substituted with, or supported by, another.³⁷⁸ Thus, even if someone could conceivably look through a crack in a closed door or a tear in a closed envelope, there are long-standing social norms against exploiting the imperfections of privacy's architecture to eavesdrop or spy. Brin himself exploits this interchangeability when he assumes that social norms will shield privacy when our technologically transformed environment no longer does so.³⁷⁹ Like norms, law can also serve as such a functional substitute for architectures of privacy—and often do so more effectively. In fact, Fourth Amendment law in particular has already been used to patch up architectural failures: it has been used to exclude observers outside a home or other private enclave from looking in when walls no longer provide a reliable shield against visual or aural spying. Thus, *Katz* forbade the use of an electronic bugging device to record the conversation within a phone booth, and *Kyllo* forbade the use of an infrared reader to build “images” of activities within a home.³⁸⁰ And while courts have not yet acted to shore up the architecture that underlies privacy and anonymity in public space, they can do so here as well.

There is a second respect in which Fourth Amendment law might bolster privacy protections eroded by new technologies. Rather than simply

government should be permitted “new powers of sight” only if it gives citizens “something in return,” perhaps including “[n]ew kinds of supervision.” *Id.* at 332. His main emphasis here is on citizens’ power to spy (with cameras) on those watching them, but he does not rule out other means of keeping government power in check. *Id.* at 333.

377. As I noted in the Introduction, this is precisely the sort of scheme that Lewis Padgett assumed might save privacy in a world in which a record of every human act is automatically etched into the structure of the surrounding physical environment. While nature enables officials to watch our entire life as though it were a movie, laws continue to forbid them from doing so.

378. See LESSIG, *supra* note 101, at 86–90 (averring that the “four modalities” of architecture, norms, laws, and markets regulate conduct both in “real space” and in “cyberspace”).

379. BRIN, *supra* note 16, at 14 (noting that people rarely stare at fellow diners in a crowded restaurant due to “[m]utual civility,” “common decency,” and a desire to avoid being “caught in the act” of staring, not because “laws require other customers to wear blinkers and blindfolds”) (emphasis omitted).

380. *Katz v. United States*, 389 U.S. 347, 353 (1967); *Kyllo v. United States*, 533 U.S. 27, 29, 34–35 (2001).

treating law as a substitute for architecture, courts can view it as a determinant of architecture. As Lessig stresses, it is a mistake to treat an architecture as an unalterable given, because laws on the Internet can reshape the basic characteristics of cyberspace, and the physical and social environment too is amenable to legislative and judicial control.³⁸¹ Often, of course, courts are less well-equipped to mandate specific changes in architecture than they are to impose specific legal prohibitions. But by making it clear, for example, that Fourth Amendment principles demand certain limits on observation, courts might spur others, including perhaps law enforcement agencies themselves, to build such constitutional limits into the technology of surveillance they use or the procedures for using it. The Supreme Court did exactly this in *United States v. Place* and *United States v. Jacobsen* by outlining a constitutional safe harbor of sorts for surveillance technologies that could narrowly reveal nothing more than specific illicit substances.³⁸² And a new Fourth Amendment jurisprudence might likewise give technology-developers and law enforcement agencies reason to build new protections into their public surveillance systems as well as those aimed at “private” spaces.

Such observations explain why courts are not helpless to repair damaged architectures of privacy. They do not, however, adequately answer another variant of the charge that an attempt to preserve privacy in public space would be backward-looking; even if it is possible for courts to put limits on public surveillance, one might argue, it is also pointless. The same technological advances that give the government the power to capture more of our lives on video also give private businesses and individuals the means to observe us as well. If the public activities we wish to hide are recorded for observation anyway—by journalists, businesses, private detectives, or random individuals—it may not seem clear what is lost by providing the same visual data to government officials, who are more accountable to us for

381. As Lessig points out, the Americans with Disabilities Act, for example, altered the built environment so as to make it more accessible. LESSIG, *supra* note 101, at 91.

382. *United States v. Place*, 462 U.S. 696, 706–07 (1982) (holding that the use of a “canine sniff” to inspect luggage suspected of containing illegal narcotics was not a search within the meaning of the Fourth Amendment because that procedure “discloses only the presence or absence of narcotics,” not more private information that might subject the property owner to “embarrassment and inconvenience”); *United States v. Jacobsen*, 466 U.S. 109, 123–25 (1983) (holding that the use of a “field test” to determine whether a white powder was cocaine was not a search within the meaning of the Fourth Amendment because the field test could only reveal “whether a substance is cocaine, and no other arguably ‘private’ fact,” meaning that the defendant’s privacy interest was “much too remote to characterize the testing as a search subject to the Fourth Amendment”). As noted in Part V, *infra*, some government authorities have already responded to similar concerns by assuring that intelligent transportation systems destroy or immediately make anonymous whatever data they collect.

the use of this information and may be more likely to use it for purposes, such as law enforcement, that serve citizens' interests. As the Court noted in *Dionisio*, "no intrusion into an individual's privacy results" when "nothing is being exposed to the grand jury that has not previously been exposed to the public at large."³⁸³

But it is one thing to give law enforcement and government the right to exploit new technologies. It is another to let a government agency stand in the shoes of private eavesdroppers. For a number of reasons, courts should be quite skeptical of the claim, frequently voiced in previous Fourth Amendment cases, that when private parties are left free to watch an individual or listen in on a conversation, government officials should be able to do so as well.

One reason for such skepticism is that whatever use private parties might make of a surveillance technique, they would find it difficult to construct as inescapable of a video surveillance system as that which the government is capable of creating. While private businesses can place camera networks on their own premises, and might even point them towards a street or highway, they do not have the authority to mount and monitor video cameras throughout a city's streets and parks. Indeed, the state's significant ability to reshape our public environment is unmatched by any other center of power in society. Thus, even those who agree with Daniel Solove that social practices which shape privacy evolve over time,³⁸⁴ and that law should respond to such evolution, might understandably reject the notion that the state should be left free to cause a sudden and seismic shift in such practices.

A second reason for applying heightened vigilance to state actors is that government can not only collect and store more information than private parties, it can also do more damage with it. While many people might be more comfortable exposing details of their lives to anonymous officials instead of people they know and interact with,³⁸⁵ the inhibitions that arise when a person knows he is being watched may well be particularly strong when he knows that the party watching him has a power, found nowhere else in society, to force him to answer questions about, or put binding limits on, his activities. While it may be particularly humiliating to have one's

383. *United States v. Dionisio*, 410 U.S. 1, 14 (1973) (citing *United States v. Doe in re Grand Jury Testimony and Contempt of Schwartz*, 457 F.2d 895, 899 (2d Cir. 1972)).

384. Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1141-43 (2002).

385. Rosen, *supra* note 139, at 49 (taking note of the observation of nineteenth-century sociologist Georg Simmel that "people are often more comfortable confiding in strangers than in friends, colleagues, or neighbors" since "[c]onfessions to strangers are cost-free because strangers move on; you never expect to see them again"). In the case of anonymous government observers who guard the secrecy of what they learn, one often never expects to see them at all.

confidences revealed to acquaintances or friends—rather than to unknown officials in a control room—one is not legally obligated to follow their rules or accept their judgments. Moreover, even recorded images are usually less threatening to privacy when no one can find them. It is true that a photo or video shot by a stranger may emerge in print, on television, or on the Internet, and cause great pain and humiliation to the subject. But often, until it does emerge, those seeking details about the subject's life will not know where to look for it. By contrast, the existence of a well-known government database of images would signal to numerous agencies and public officials that there is a place to find such information, and perhaps give private parties the incentive to lobby vigorously for access to it.³⁸⁶

There is a third reason to draw a distinction between videotaping by private parties and videotaping by government. The balance we are trying to strike in each case is an entirely different one. In formulating regulations for private use of cameras and video cameras, the balance is generally one between freedom and privacy. We often tolerate videotaping by private parties, and the potential sacrifice of privacy it entails, because placing significant restraints on when people can take pictures of us would cut significantly into their freedom, and ours. Public life would certainly be more suffocating if we could only use a camera or video camera in a public street or park at the risk of being sued by someone we happen to catch on film, or prosecuted at that person's request. We also balance other values against privacy—for example, the convenience of “targeted” services—but respect for individual freedom is likely to be the major constraint on what legal restrictions society can adopt to protect our privacy against observation by fellow citizens. In contrast to constraints on individuals, constraints on government authorities do not typically come at the cost of individual freedom.³⁸⁷ On the contrary, such constraints are part and parcel of a political regime organized around the notion of limited government.

386. The experience with electronic toll ways lends credence to fears that numerous parties who have reason to pierce individuals' privacy would be more likely to do so if they knew of a central government storage unit where such information could be found: as noted above, agencies and private parties have subpoenaed records from Illinois' I-Pass systems for reasons that have nothing to do with assuring payment of tolls or monitoring traffic. *See supra* section II(B)(I). Robyn Moo-Young discusses the benefits of decentralization in her analysis of how biometric technologies might be used in the banking industry:

[K]nowing that there is *not* one centralized government storage area could ease consumer fears. Since there is no main warehouse where all biometric information is stored, storage is most often on the unit, local server, or a remote server intended for a single application. Because companies would all have their own systems, it would be difficult for perpetrators to crack the codes or decipher the algorithms.

Moo-Young, *supra* note 261, at 449 (emphasis added).

387. As Joseph Raz points out, unlike “corporations and voluntary associations,” which may have “independent interests,” “political authorities . . . do not have a legitimate interest of their

Constraints on government activity might still be unwise or damaging, not because it is inherently objectionable to limit the freedom of accountable public officials, but rather because one could conceivably undercut their ability to do the tasks that society relies on them to do—enforce the law, protect public safety, and effectively run schools and other public institutions. In some cases, to be sure, we may need to grant them powers that ordinary citizens do not have. For example, police are permitted, pursuant to a warrant, to intercept electronic communications that a private party or business is not allowed to intercept under any circumstances for its own purposes. But even these special grants of monitoring power to law enforcement generally come with strict limits, either in the form of a warrant or a “warrant substitute,” designed to prevent this surveillance power from being abused.³⁸⁸

For all these reasons, it is wrong to think that courts would place unacceptable constraints on law enforcement, or would be attempting to freeze technological progress or societal change, by adopting a Fourth Amendment jurisprudence that protected core privacy-protecting features of public space. On the contrary, by providing assurances that law enforcement’s use of technologies remains consistent with core privacy values, such a Fourth Amendment jurisprudence may well give law enforcement greater freedom to exploit new technologies than they would otherwise be allowed. Police and other officials may well find it easier to experiment with new law enforcement technologies if they are first given ground rules, like those in the Wiretap Act, for how to do so in a manner consistent with core constitutional privacy values. Citizens may be more likely to trust such experiments knowing that ground rules exist to keep them within constitutional boundary lines.³⁸⁹

own” but must pursue only the interests of their subjects. JOSEPH RAZ, *THE MORALITY OF FREEDOM* 5 (1986).

388. See *infra* Part V.

389. As Eugene Volokh notes, “[c]onstitutional constraints . . . are thus not only legislation-frustrating . . . but also in some measure legislation-facilitating,” because those who would otherwise oppose a measure in its entirety may accept it if it is limited by constitutional constraints and they know it cannot be converted into a more intrusive government intervention. Eugene Volokh, *The Mechanisms of the Slippery Slope*, 116 HARV. L. REV. 1026, 1047 (2003). Indeed, Volokh mentions video surveillance as one area in which worries about a “slippery slope”—e.g., the installation of face recognition technology on cameras or permanent recording of what the cameras observe—could lead citizens to oppose surveillance they would otherwise accept, and in an area which it may therefore be valuable to have constitutional limits that prevent slipping. *Id.* at 1041.

IV. Applying Privacy Protections to Public Space: Revising *Katz* and Refining Justice Harlan's Alternative Framework

There is another objection one might make to a Fourth Amendment jurisprudence centered largely on preserving the architecture of privacy—that it is unnecessary. Instead of replacing the *Katz* test, we might try to salvage it. Many commentators have argued that *Katz*, correctly interpreted, should extend Fourth Amendment protection against monitoring of our public movements.³⁹⁰ Thus, former Canadian Supreme Court Justice Gérard La Forest has argued that Section 8 of the Canadian Charter does not “demarcate rigid, formalistic borders between private and public spatial domains” and that courts can continue to anchor privacy protection by identifying what constitutes a “reasonable expectation of privacy in a given context.”³⁹¹ Christopher Slobogin has shown that unconstrained public video surveillance is at odds with empirical evidence about Americans’ expectations of privacy.³⁹² The Hawaii Supreme Court in *Bonnell* likewise hinted that one might ground privacy protections in public places on the legitimate “expectations of privacy” that we bring there.³⁹³ Such an approach, one might argue, allows courts to meet the challenge of extending privacy to public life without abandoning the important and helpful precedent generated under the *Katz* test.

Such precedent is valuable in large part because any overarching alternative to the *Katz* test of what counts as a “search” is likely to be an abstract one in need of elaboration. The Harlan or Amsterdam alternative to the *Katz* test is no exception: in asking “whether the amount of privacy and freedom remaining to citizens would be diminished to a compass inconsistent with the aims of a free and open society” if a “particular form of surveillance is” left constitutionally unregulated,³⁹⁴ courts would have to struggle with

390. See, e.g., Mathew Mickle Werdegar, Note, *Lost? The Government Knows Where You Are: Cellular Telephone Call Location Technology and the Expectation of Privacy*, 10 STAN. L. & POL’Y REV. 103, 111 (1998) (arguing that the expectation of privacy in one’s public movements is a fundamental cultural belief and thus, contrary to *Smith v. Maryland*, does satisfy the *Katz* test); Melvin Gutterman, *A Formulation of the Value and Means Models of the Fourth Amendment in the Age of Technologically Enhanced Surveillance*, 39 SYRACUSE L. REV. 647, 706 (1988) (analogizing the “continuous use of a modern, sophisticated tracking device to record every public movement” to the monitoring of a phone call at issue in *Katz* and concluding that the former is unconstitutional under the *Katz* rationale).

391. Letter from Justice Gérard La Forest, former Canadian Supreme Court Justice, to George Radwanski, Privacy Commissioner of Canada, at notes 22–24 and accompanying text (Apr. 5, 2002), at http://www.privcom.gc.ca/media/nr-c/opinion_020410_e.asp.

392. Slobogin, *supra* note 38, at 272–85.

393. See *State v. Bonnell*, 856 P.2d 1265, 1275 (Haw. 1993) (“Accordingly, the test is one of reasonable expectations of privacy. Every individual has expectations of privacy with regard to his person wherever he may go, be it a public park or a private place . . .”).

394. Amsterdam, *supra* note 355, at 403.

what this language means. What amount of privacy and freedom does a free society require? How does one define the particular “form of surveillance”? For example, when police use a crude video camera to tape a suspect, is the “form of surveillance” simply the use of a single crude camera, or must courts instead come to a conclusion applicable to all types of video surveillance, including extensive networks of powerful cameras?

Rather than confront such difficult questions and build a new Fourth Amendment jurisprudence from the ground up, one might argue that we should first try to address new problems within the framework already developed over the past thirty-seven years by courts under the “reasonable expectations of privacy” test. It is certainly possible to make a persuasive case for “public privacy” under the reasonable expectations test. The language of “reasonable expectations” is broad enough to accommodate such an expansion of Fourth Amendment rights. However, such a route is an imperfect and in some respects misleading one, because the core purpose of the Fourth Amendment’s privacy protection is not to honor expectations, but to preserve opportunities. Just as the First Amendment preserves “spaces” for dissent, even for those who are currently uninterested or unaware of such spaces, the Fourth Amendment should be understood as preserving similar spaces for private and anonymous action.

The somewhat deceptive nature of the *Katz* framework has already been acknowledged in many courts’ dismissive treatment of a central component of that framework. Although Justice Harlan made an “actual (subjective) expectation of privacy” the first requirement for Fourth Amendment protection in his two-prong *Katz* test,³⁹⁵ various commentators³⁹⁶ and courts have since appeared to give it little weight. As the Supreme Court itself pointed out in *Smith v. Maryland*, putting weight on actual expectations could result in absurd consequences: “[I]f the Government were suddenly to announce on nationwide television that all homes henceforth would be subject to warrantless entry, individuals thereafter might not in fact entertain any actual expectation of privacy regarding their homes, papers, and effects.”³⁹⁷

Even absent government manipulation, moreover, it is not clear why an expectation of privacy should be a prerequisite to Fourth Amendment protection. 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

395. *Katz v. United States*, 389 U.S. 347, 361 (1967).

396. See, e.g., Heffernan, *supra* note 116, at 36 (noting that, perhaps in response to the absurd results it justified, “the Court has not treated the first prong [of the *Katz* test, the subjective expectations test,] as a key element of its post-*Katz* jurisprudence” and that it has been of “marginal importance”).

397. *Smith v. Maryland*, 442 U.S. 735, 740 n.5 (1979).

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? Thus, as the Supreme Court also noted in *Smith*, "if a refugee from a totalitarian country, unaware of this Nation's traditions, erroneously assumed that police were continuously monitoring his telephone conversations, a subjective expectation of privacy regarding the contents of his calls might be lacking as well."³⁹⁸ Still, the Court would enforce his Fourth Amendment rights against warrantless wiretapping.

Perhaps for these reasons, courts analyzing video surveillance have sometimes passed over the first prong with virtually no analysis. In one case where a video camera was mounted in plain view above the sidewalk, the court nonetheless "assum[ed] *arguendo*, that Defendant had an actual, subjective expectation of privacy" and proceeded to the objective reasonableness inquiry, which it noted was "the crux of the privacy test."³⁹⁹ Another court was likewise "willing to assume *arguendo* that the appellants, as they profess, had some subjective expectation of privacy while at work,"⁴⁰⁰ even though the employees bringing the case were informed "in advance that video cameras would be installed and [the employer] disclosed the cameras' field of vision."⁴⁰¹

If the "reasonable expectations" test has value for Fourth Amendment analysis, it is not because subjective expectations matter, but rather because the notion of a "reasonable expectation of privacy," while somewhat vague, provides a conceptual tool that courts can use to organize what would otherwise be a chaotic and intricate multi-factor analysis. Privacy, many writers have noted, is an extraordinarily complex concept,⁴⁰² and a justified sense of privacy can arise from many different elements of a situation, including the nature of the place one is in, the nature of the activity one is conducting, or with whom one is interacting. Faced with such complexity, judges might find it invaluable to have a thought experiment of the sort suggested by the "reasonable expectation of privacy" test, which they can use to identify and tie together all the relevant factors present in a given situation.

398. *Id.* at 740-41 n.5.

399. *State v. Augafa*, 992 P.2d 723, 733 (Haw. Ct. App. 1999).

400. *Vega-Rodriguez v. P. R. Tel. Co.*, 110 F.3d 174, 178 (1st Cir. 1997).

401. *Id.* at 180. The court factored this notice into its analysis in applying the objective reasonableness prong of the *Katz* test. It recognized the fact that notice was related to subjective expectations and stressed, "we do not mean to imply that an employer always can defeat an expectation of privacy by pre-announcing its intention to intrude into a specific area." *Id.* at 180 & n.4.

402. Solove, *supra* note 384, at 1088-89 (noting that numerous "philosophers, legal theorists, and jurists have lamented the great difficulty in reaching a satisfying conception of privacy" and citing numerous writers who place emphasis on its complexity).

They can ask whether there are elements in this situation that would lead a reasonable person to expect privacy, and identify, for the benefit of the parties, the police, and future courts, what these elements are. The open-endedness of the concept of a “reasonable expectation of privacy” also allows room for adjusting our Fourth Amendment analysis to accommodate new understandings of, or changes in, the types of circumstances that give rise to privacy.⁴⁰³

The problem with such a multi-factored approach is that it inevitably weakens the extent to which citizens can rely on the sheltering features of private and public spaces. As Michael Adler has pointed out, the home becomes a less certain sanctuary when courts identify factors apart from location that can, individually or in combination, make in-home activity “nonprivate”—when, for example, the nature of a specific activity in the home makes it an acceptable target for focused surveillance.⁴⁰⁴ The same can be said about the privacy-protecting features of public spaces. Even law-abiding individuals cannot have significant confidence in the anonymity or privacy they find in public spaces if a multitude of other considerations, for example, the “nonintimate” nature of the activity, are deemed by courts to transform them into fair targets for surveillance. This does not mean that courts should ignore the complexity of striking a proper balance between privacy and security under the Fourth Amendment. But such balancing will be more likely to honor core constitutional commitments rooted in “the aims of a free and open society” if it first recognizes the importance that certain spaces, and features of those spaces, have for privacy, and postpones for the “reasonableness” analysis the complicated question of when government entry into, or monitoring of, such spaces is nonetheless justified (perhaps because of the dangerous acts that might take place there, or perhaps because other powerful considerations of public interest require that the government monitor behavior there in limited ways).

Nonetheless, even under the vague language of the “reasonable expectations” test, courts might organize their Fourth Amendment inquiry in

403. A number of writers emphasize that the nature of privacy shifts as society changes. *E.g.*, *id.* at 1141–43. Christopher Slobogin makes a similar point, noting that if expectations of privacy with respect to a particular surveillance method change, the “Fourth Amendment analysis should probably change with them.” Slobogin, *supra* note 38, at 281. Much in the way that John Locke’s notion of “substance” allowed us to acknowledge that there might be properties of a particular material (e.g., gold) beyond those which we currently recognize with our senses (e.g., its color and texture) in a particular circumstance, one might argue that because of its open-endedness, the reasonable expectations test allows room for sources of privacy not yet obvious to us. *See* JOHN LOCKE, AN ESSAY CONCERNING HUMAN UNDERSTANDING, bk. II, ch. XXIII, §§ 10–12, at 301–03 (Peter H. Niddich ed., Oxford Univ. Press 1975) (1690).

404. Adler, *supra* note 288, at 1111–12.

a way that recognizes the importance of the privacy-protecting features of public space. They might do so, for example, by applying to public space a rebuttable presumption modeled on that which *Katz* provides in more familiar settings for private activity, such as the home. Rather than assuming that every activity in a home is private, *Katz* held that “[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.”⁴⁰⁵ As the Second Circuit noted in *Taborda*, this holding effectively transformed the assumption that in-home activity was private into a rebuttable presumption, which an investigator could overcome by showing that the in-home activity observed was “knowingly expose[d].”⁴⁰⁶ One way courts might recognize a right of privacy even in public and observable activities is by transforming the assumption that a public and observable activity is unprotected into a rebuttable presumption as well. This would allow people to show, for example, that while an activity took place in a park or street, it took place under conditions which made it reasonable to expect it would not be observed or videotaped (or used as a foothold by which authorities could gain a deeper view of an individual’s life). When public video surveillance locks onto and tracks an individual, or peers invisibly over his shoulder at documents he would otherwise have reason to believe no one could see, he might well have grounds to rebut the assumption that the public setting of his activity meant that it was exposed to the world.

In inquiring into whether a rebuttable presumption of “publicness” has been overcome, courts applying the *Katz* test would likely draw upon the kinds of factors that Christopher Slobogin has identified as important when the place of the observation is not itself determinative.⁴⁰⁷ Slobogin lists six factors, apart from the place of the surveillance, which courts have used in applying the *Katz* test: (1) the location of the observer, especially whether he is intruding on private property; (2) the precautions taken by the observed individual to protect his privacy; (3) whether the surveillance technology replaces or simply enhances the natural senses; (4) whether that technology is

405. *Id.* at 1104.

406. *See* *United States v. Taborda*, 635 F.2d 131, 138 (2d Cir. 1980). The court stated:

The very fact that a person is in his own home raises a reasonable inference that he intends to have privacy, and if that inference is borne out by his actions, society is prepared to respect his privacy. But the inference *may be rebutted* by the person’s own actions. If in his home he conducts activities or places objects in such a way that the activities or objects are seen by the unenhanced viewing of persons outside the home, located where they may properly be, such observations transgress no Fourth Amendment protection

Id. (emphasis added) (footnotes omitted).

407. *See* Slobogin, *supra* note 325, at 390–98.

generally available to or in “general use by” the public; (5) the steps taken by observers to minimize the intrusion by their surveillance; and (6) the nature of the object or activity observed by the surveillance.⁴⁰⁸

Unfortunately, as Slobogin himself observes, most of these factors are of little value in determining whether the Fourth Amendment should apply to any given surveillance technology.⁴⁰⁹ Moreover, their relevance is even more questionable with respect to public cameras in particular. The first factor, location of the observer, is clearly of little value: government cameras hardly need to intrude on private areas to tape activities visible in public places. The second, precautionary measures, is of value only when one could conceivably protect one’s privacy against the surveillance technique in question, and it is hard to imagine how one might do this in streets where cameras are ubiquitous. While one could conceivably wear masks, and some antisurveillance protesters have experimented with devices that “blind” the cameras,⁴¹⁰ these are hardly realistic proposals for shielding one’s day-to-day activities.⁴¹¹

As Slobogin points out, the third factor—whether the surveillance technology enhances or replaces the natural senses—seems to be based on a “false distinction.”⁴¹² Every technology that police use to aid their surveillance in some manner *replaces* senses by giving police access to information they could not otherwise obtain.⁴¹³ When a person’s hidden or secluded activity is recorded for others to view, it makes little difference whether the acts were captured by a machine that records light waves (which the human eyes can sense) or one that records heat (which they cannot). The intrusion into the person’s informational privacy is the same in both cases.

408. *Id.* He mentions only “the place observed” and “minimization” as “central to any analysis of physical surveillance technology.” *Id.* at 398.

409. *Id.* at 398–401.

410. See John Markoff, *Protesting the Big Brother Lens, Little Brother Turns an Eye Blind*, N.Y. TIMES, Oct. 7, 2002, at C1 (describing how one opponent of public video surveillance is using “inexpensive laser pointers to temporarily blind those omnipresent electronic eyes”).

411. One could also invest some time in creating a false picture of one’s life, but this is not a burden an individual should have to undertake to protect privacy. As Anthony Amsterdam has said with respect to other precautionary measures: “[A]nyone can protect himself against surveillance by retiring to the cellar, cloaking all the windows with thick caulking, turning off the lights and remaining absolutely quiet. This much withdrawal is not required in order to claim the benefit of the amendment because, if it were, the amendment’s benefit would be too stingy to preserve the kind of open society in which we are committed and in which the amendment is supposed to function.” Amsterdam, *supra* note 355, at 402. The same could be said of wearing a hat and sunglasses everywhere, having to act at odds with one’s actual feelings, or any of the measures that might be conceivably effective in rescuing some of one’s privacy in public places watched by surveillance cameras.

412. See Slobogin, *supra* note 325, at 400.

413. See *id.* (“Presumably, if the enhancement device does not in some way ‘replace’ police vision, it will not be used in the first place.”).

I have already briefly discussed the fourth factor, namely, the extent to which surveillance technology is “generally available” or in “general public use.”⁴¹⁴ As Slobogin points out, this factor is also suspect, because “giving full weight to this factor would eliminate privacy expectations even in much of the home because so many highly intrusive devices (e.g., \$22,000 map-making cameras) are readily ‘available’ to the public.”⁴¹⁵ Even when certain technologies, like tape recorders or binoculars, are available and widely-used, this has not stopped courts from imposing constitutional limits on how such technologies can be used. To the extent this factor has any value at all, however, it seems to provide courts with reason to at least be suspicious of public video surveillance, because although video cameras are themselves pervasive, wide-scale networks of linked cameras, covering huge portions of public space, are not in general public use.

This leaves only two factors: (a) the nature of the activity to be observed and (b) minimization of the intrusion. Not surprisingly, given the irrelevance of the other factors, these are the two factors that the Supreme Court has mentioned in dicta as providing a possible basis for applying the Fourth Amendment to surveillance in public places. In *Dow Chemical*, the Court suggested that the constitutionality of surveillance may depend on the nature of the activity observed.⁴¹⁶ Chief Justice Burger stated for the Court that the Fourth Amendment was not implicated when EPA agents photographed the outside of a chemical plant from public airspace, but he suggested that the result might be different if the agents photographed “intimate details.”⁴¹⁷ In *Ciraolo*, the Court likewise noted that aerial observation might constitute a search if it revealed “those intimate associations, objects or activities otherwise imperceptible to police or fellow citizens.”⁴¹⁸ As noted earlier, the Court’s wiretap analysis in *Berger* already required “minimization” as a condition of a warrant,⁴¹⁹ and Justice Rehnquist was arguably relying on the logic of the minimization argument when he noted in *Knotts* that the Constitution might bar the use of tracking technology to conduct “twenty-four hour surveillance” of citizens’ movements.⁴²⁰

But these two factors do not capture what it is that makes video surveillance so intuitively troubling and in need of constitutional regulation. The “intimate activities” test, as I have argued above, invites judges to make controversial judgments about what individuals do and do not deserve to

414. See *supra* subpart III(C).

415. Slobogin, *supra* note 325, at 399.

416. *Dow Chem. Co. v. United States*, 476 U.S. 227, 238 (1986).

417. *Id.* at 238 & n.5.

418. *California v. Ciraolo*, 476 U.S. 207, 215 & n.3 (1986).

419. *Berger v. New York*, 388 U.S. 41, 57, 59–60 (1967).

420. *United States v. Knotts*, 460 U.S. 276, 283–84 (1983).

keep private. These judgments may well depend on information about an individual's life that courts do not have and which would require further intrusion into that person's privacy to obtain. In any case, it is not the nature of the activities observed by video surveillance that makes such surveillance so troubling, but the extent to which it changes the nature of the public space and deprives it of the qualities that make it a promising site for anonymous, private, or spontaneous action.⁴²¹

The "minimization requirement" takes better account of video surveillance's impact on the surrounding environment. But it cannot by itself explain why dragnet surveillance might count as a "search" when the government points to a compelling need for it. If the government claims that certain forms of suspicionless investigation (mass video surveillance, for example) are necessary to battle terrorism, then one does not refute the argument by merely demanding that the search technique go no further than necessary. Moreover, an argument that investigators should minimize a certain sort of monitoring has little force unless one first explains why "too much" monitoring counts as "too much." Without such an explanation, a minimization test simply invites judges to assume that they "know" an excessively broad search "when [they] see it,"⁴²² without giving guidance as to what makes such a search excessively broad. Courts also need some way of telling whether minimization exempts a particular form of surveillance from Fourth Amendment constraints entirely, or simply renders it "reasonable" and thus permissible so long as it occurs under additional constraints, like limitations on the purpose for which the technique may be used.

Courts might perhaps salvage the "intimate facts" or "minimization" tests by extricating them from the vague language of reasonable expectations of privacy—and legal scholars and courts have explored such a possibility. For example, instead of charging judges with the impossible task of defining what public information should count as intimate, some scholars have, in a sense, made this decision for courts and thus simplified their mission. Courts, they argue, should firmly protect people's private communications. Edmund Kitch, for example, suggests that police should be barred not only from eavesdropping on a person in a phone booth, but also from covering a public park with sensitive microphones or installing an electronic listening device in a public restaurant.⁴²³ Elaborating upon this proposal, Wayne LaFare argues that perhaps the Fourth Amendment should apply with special

421. See *supra* subpart III(B).

422. This approach has been advanced in another area of constitutional jurisprudence: Justice Potter Stewart declared in *Jacobellis v. Ohio* that although he could not define "hard-core" pornography, "I know it when I see it." 378 U.S. 184, 197 (1964).

423. See Kitch, *supra* note 101, at 139–40.

force to *communication* that takes place in public, but not to all other activity that occurs in open spaces.⁴²⁴ In a similar vein, David Sklansky argues that the key lesson that the current Court should distill from *Katz* is that “the privacy protected in *Katz* attached neither to a person (Charles Katz), nor to a place (the telephone booth), but to a communication (the telephone conversation). Katz had a reasonable expectation of privacy neither because of who he was nor because of where he was, but because of what he was doing.”⁴²⁵ Such proposals substitute a bright line for what would otherwise be a slippery “intimate facts” test.

And courts have recently hinted at a similar refinement of the “minimization” test, holding that officials come under the bounds of the Fourth Amendment when their observation moves from casual observation of identified strangers to sustained scrutiny, tracking, or identification of a particular individual. In *United States v. Taketa*, for example, the Ninth Circuit found that video monitoring violated a defendant’s Fourth Amendment rights in large part because the camera was aimed at the defendant, and not simply the place he was in, and because the “silent, unblinking lens of the camera was intrusive in a way that no temporary search of the office could have been.”⁴²⁶ All of these factors seem to be rooted in the same concern: video surveillance is damaging when it is used to track specific individuals, rather than simply capture information about places, events, or crowds. “Minimization,” on this view, might demand first and foremost that police not use cameras or other monitoring technologies to hone in on and follow individuals whom they have no reason to suspect of a crime.⁴²⁷

Even when recast in this way, however, such elements of the “reasonable expectation” test are insufficient by themselves to protect the core privacy interests threatened by video surveillance: individuals reveal many clues about their interests or activities even when they are not communicating with each other. And video surveillance systems could do significant damage to their privacy by capturing and archiving their movements through public space, even before such archives are consulted by

424. See LAFAVE, *supra* note 52, § 2.2(e), at 443 (“[T]here is more reason to protect the expectation that one can converse in private when no one else is in hearing range than there is to protect the expectation that public conduct will be unobserved when no one is within range to see it with the naked eye.”).

425. Sklansky, *supra* note 102, at 195.

426. 923 F.2d 665, 677 (9th Cir. 1991); see also cases discussed *supra* subpart II(A).

427. As noted in subpart II(A), the Ninth Circuit, despite its *Taketa* decision, has refused to apply such a minimization principle to surveillance of streets, parks, or other public places. The Supreme Court, likewise, has apparently held that police observation in public is unconstrained by this variant of the minimization standard: its decision in *Knotts* imposed no constitutional limits on how closely police might track individuals on public roadways. *United States v. Knotts*, 460 U.S. 276 (1983).

any official interested in their individual activities. What courts and legal scholars need, therefore, is jurisprudence that not only allows people to have unmonitored conversations in public parks and to avoid being systematically tracked from street to street, but which does so as part of a more comprehensive effort to recognize and protect the importance of privacy and anonymity in public life.

Courts might find a starting point for such an effort in the analysis outlined earlier in Part III: the kind of twenty-four hour surveillance that seemed to trouble the Court in *Knotts*⁴²⁸ and the kind of identity-revealing magnification that troubled the Court in *Dow Chemical*⁴²⁹ are troublesome not simply because they are excessive in some unspecified way or focus too closely on individuals, but rather because they break down, and do not replace core features of the architecture of privacy in public life. They transform the environment in such a way that, to use the terminology used by Amsterdam, the “privacy and freedom remaining to citizens would be diminished to a compass inconsistent with the aims of a free and open society.”⁴³⁰

Admittedly, Amsterdam’s test is not self-interpreting. Courts and citizens need to be able to draw practical and relatively consistent conclusions about when privacy and freedom are “diminished to a compass inconsistent with the aims of a free and open society.”⁴³¹ This is not a straightforward mission. Different citizens and judges may well disagree over just how much freedom from monitoring a free society needs. Perhaps it is for this reason that Amsterdam concludes that while the effect of a surveillance technique on freedom is the “ultimate question” in identifying a Fourth Amendment search, “it is a perfectly impossible question for the Supreme Court to put forth as a test of fourth amendment coverage.”⁴³² Rather, he noted, this question can be answered only if it is “transmuted” into a framework that is more administrable.⁴³³ Amsterdam himself, and many courts that have approved of his formulation, have suggested that this more administrable framework might be found in *Katz*’s reasonable expectations test.⁴³⁴ But “reasonable expectations of privacy” are also difficult for judges

428. *Id.* at 283–84.

429. *Dow Chem. Co. v. United States*, 476 U.S. 227, 238–39 (1986).

430. *See* Amsterdam, *supra* note 355, at 403.

431. *Id.*

432. *Id.*

433. *Id.* at 404.

434. *See id.*; *see also, e.g.*, *Florida v. Riley*, 488 U.S. 445, 456 (1989) (Brennan, J., dissenting) (treating the Amsterdam test not as an alternative to the *Katz* test, but as identifying the key consideration for determining what privacy expectations count as reasonable or legitimate); *United States v. Hendrickson*, 940 F.2d 320, 322 (8th Cir. 1991) (same).

to identify—and for the reasons I have already given, the *Katz* test blinds judges to the privacy-corroding impact of many forms of public surveillance.

A more promising approach is to give more definite shape to the Amsterdam test by highlighting the hard-to-discern architecture of privacy that must be protected if Americans are to remain sufficiently free from monitoring in public spaces. While it might require some time (and some years of judicial interpretation) to trace the contours of this architecture, courts might at least begin doing so by protecting certain features of public space that intuitively seem to provide crucial support for the freedom modern individuals find in streets and public spaces: (1) the *seclusion*, and freedom from close scrutiny, we can find even in public spaces, by putting distance between ourselves and other observers or shielding our activities (for example, the reading of a book or letter) behind natural or artificial barriers in parks or squares; (2) the *anonymity* we expect to find in public settings where people cannot identify us by name; (3) the ability to *compartmentalize* our lives, by preventing those in one social environment from learning about interests, beliefs, or plans we reveal in another; (4) the *casualness and unthreatening* nature of the scrutiny we generally expect to find in public places, where we are often ignored by others around us and often perceived only as an undifferentiated element of the surrounding social environment; and (5) the *impermanence* of the numerous spontaneous statements or acts in which we engage in public environments, with confidence that they will not “define” us for everyone we subsequently encounter. Judicial attention to these factors would provide more solid protection for “public privacy” than the controversial and often confusing factors that courts have drawn upon in the past to identify “reasonable expectations of privacy.”

Even if courts can agree on the architecture of privacy that must be protected from surveillance, it is also no easy matter to define, in each case that comes before a court, the “form of surveillance” that is to be evaluated in light of its effect on this architecture. Consider the one state case to expressly apply the Amsterdam or Harlan model to video surveillance in a public area. In *Cowles v. State*, the Alaska Supreme Court asked itself whether leaving authorities free to engage in video surveillance of a university employee suspected of theft would leave citizens vulnerable to more surveillance than was acceptable in a free society.⁴³⁵ The court found that it would not be, largely because authorities used video surveillance to observe only one person who they had already suspected of theft based on other information.⁴³⁶ The “form of surveillance,” assumed the court, included only what the police actually did, not what they might do with more advanced

435. *Cowles v. State*, 23 P.3d 1168, 1171 (Alaska 2001).

436. *Id.*

versions of the same technology (such as modern networks including hundreds or thousands of cameras). In asking whether the form of surveillance cut too deeply into privacy, the court defined “form of surveillance” quite narrowly. This is certainly one way in which courts might define a “form of surveillance” under the Harlan or Amsterdam test. But one might also define it more broadly, as the Supreme Court did in *Kyllo*.⁴³⁷ Although acknowledging that the infrared technology used in the case itself was “relatively crude,” it insisted that “the rule we adopt must take account of more sophisticated systems that are already in use or in development.”⁴³⁸ As these cases demonstrate, courts have plenty of room to maneuver in applying the Harlan or Amsterdam test.

Of course, courts can decide for themselves how narrowly to define a particular technique in applying the Harlan or Amsterdam test. But both low and high levels of abstraction lead to predictable problems. On the one hand, if courts follow the example of the Alaska Supreme Court in *Cowles* and use only narrow definitions of a particular technique, tied tightly to the specific facts of the case,⁴³⁹ they will provide little guidance for courts analyzing that technology in other circumstances and little guidance for government officials and citizens trying to figure out how the use of a surveillance technique is constrained by the Fourth Amendment. As the Supreme Court indicated in *Kyllo*, such a time-bound view might well leave citizens at “the mercy of advancing technology.”⁴⁴⁰ On the other hand, if courts analyze surveillance techniques at the highest level of abstraction, they may overlook limitations on the technology that render it clearly unthreatening to privacy. Even simple visual inspection by the police, without any technological enhancement, could limit “the amount of privacy and freedom . . . to a compass inconsistent with the aims of a free and open society.”⁴⁴¹ A society where an army of policemen intensively scrutinize every passerby at every street corner would probably not fit most Americans’ conception of what a free society looks like, but this does not mean that any visual inspection by a policeman in a public place should count as a Fourth Amendment “search.”

There is, however, a way out of this dilemma: the Fourth Amendment inquiry into what constitutes a “search” could combine the broader and narrower views of a certain surveillance technology in a way that takes account of the value that each of these perspectives has for understanding the

437. *Kyllo v. United States*, 533 U.S. 27, 40 (2001).

438. *Id.* at 36.

439. See *Cowles*, 23 P.3d at 1175 (limiting the holding of the case to surveillance of public employees where there is a legitimate purpose or reasonable cause).

440. *Kyllo*, 533 U.S. at 35.

441. *Amsterdam*, *supra* note 355, at 403.

danger posed by such a technology. First, courts might begin by taking a broader view and presumptively classifying as a “search” the use of any surveillance technology which, considered at a high level of abstraction, has significant potential to pierce, circumvent, or erode any feature of public or private space that protects private or anonymous action. In a sense, this is what the Supreme Court did with respect to wiretapping in *Berger v. New York*, when it considered what type of statute is necessary to make use of such technology safe for constitutional democracy.⁴⁴² It stressed that “[b]y its very nature eavesdropping [whether by wiretapping or other devices] involves an intrusion on privacy that is broad in scope,” and that special safeguards are therefore generally necessary.⁴⁴³

There is little question that, like wiretapping and electronic eavesdropping, video surveillance, use of a beeper or similar tracking device, and use of infrared technology all present potentially serious threats to privacy. All of these technologies, after all, are designed to allow police or other investigators to overcome the barriers or cross distances that citizens have long relied upon to block external monitoring of their activities. By contrast, when police use only their unaided vision to observe activities in public spaces, courts might begin with the opposite presumption because simple visual observation does not usually overcome privacy-protecting barriers unless the state takes elaborate measures to assure it can do so, such as putting an official observer at every corner.

Having begun by asking when a certain technology, considered in the abstract, presents a threat to privacy, courts might then take a narrow look at the specific manifestation of the surveillance technique they are examining to see whether any aspects of this particular surveillance activity should lead them to abandon their initial presumption. Thus, when police use only their eyesight, but subject citizens to suspicionless, close, and continuous scrutiny, then this may constitute a search even if unaided visual observation normally does not.⁴⁴⁴ When a specific use of video surveillance involves only the use of a single camera to provide only a brief snapshot of a few suspect

442. *Berger v. New York*, 388 U.S. 41, 58–60 (1967) (critiquing the New York eavesdropping statute as a blanket grant of permission that lacks adequate judicial supervision and Fourth Amendment protective procedures, such as requiring officers to particularly describe the information sought, promptly execute the warrant, and notify suspects of the search).

443. *Id.* at 56 (emphasis added).

444. As Lee Milstein emphasizes, while the Fourth Amendment constrains the scanning of homes or suitcases with thermal imagers, your privacy is more damaged when a police officer follows you around and “write[s] down the name of every location you visit and the name of every person with whom you interact.” Lee C. Milstein, Note, *Fortress of Solitude or Lair of Malevolence? Rethinking the Desirability of Bright-Line Protection of the Home*, 78 N.Y.U. L. REV. 1789, 1789 (2003).

transactions, a court might conclude that it is not eroding or circumventing the features of public space that provide opportunities for anonymous or private action, even if video surveillance might easily do so when used on a more massive scale. Even technologies that seem threatening to privacy (such as thermal imaging) might be rendered less threatening by built-in technological protection: as Lee Milstein notes, while the *Kyllo* majority focused on how developments in a certain technology might undercut privacy, such developments might also generate effective and novel ways of protecting it.⁴⁴⁵

However, because a nonsearch is completely outside the bounds of the Fourth Amendment, courts should be hesitant to place a potentially powerful surveillance technique in this category. They should not do so unless they are quite sure that the use of such a technology is limited by firm constraints that eliminate virtually all threats it might present to the integrity of our private and public spaces. Consequently, courts should rethink the decisions that give such surveillance technologies the benefit of the doubt or that classify them as nonsearches on the basis of constraints that investigators can overcome with little effort. They might rethink, for example, the Supreme Court's conclusion in *Karo* that installation of a beeper in a person's property does not by itself trigger the Fourth Amendment, because a beeper can transmit no information about a person until it is turned on.⁴⁴⁶ The problem with this reasoning is that even if the beeper remains off, its mere presence in someone's property has made him significantly more vulnerable to observation than he was before. The only barrier preventing a beeper from being used to its full privacy-invading potential might be overcome with a flick of a switch.

A similar analysis also would have been helpful in *United States v. Place*⁴⁴⁷ and *United States v. Jacobsen*.⁴⁴⁸ instead of simply concluding that

445. *Id.* at 1816–17 (arguing that “advancements in technology are as likely to help protect privacy as invade it” and noting that advances in thermal imaging technology might produce more invasive forms of it, but could also result in thermal imagers that “remove the pictures from the read-outs altogether, analyze the exact wavelength of the heat emanating from the house and indicate only when halide lamps are being used to grow plants with certain characteristics of marijuana plants”); see also *infra* note 560 (discussing versions of face recognition technology allowing police to learn useful facts that might be of law enforcement interest without piercing individuals' anonymity).

446. *United States v. Karo*, 468 U.S. 705, 712 (1984).

447. 462 U.S. 696, 707 (1983) (concluding that because a “canine sniff” allows luggage to remain closed and the dogs are trained to detect only the presence of narcotics, the procedure is sufficiently limited and therefore is not a search).

448. 466 U.S. 109, 123–24 (1984) (holding that a chemical field test that is designed so that it merely indicates whether or not a given substance is cocaine does not invade any legitimate privacy interest and thus is not a search).

existing limitations on dog sniffs or drug tests automatically render them nonsearches, the Court might have also examined, as the Court *did* in *Kyllo*,⁴⁴⁹ whether these methods for detecting substances might be easily transformed into techniques that reveal not merely whether someone possesses illicit or dangerous substances, but also other, more innocent details about individuals.⁴⁵⁰

Defining a “search” in this admittedly broad way helps to clarify the respective roles of the “search” and “reasonableness” inquiries in the larger Fourth Amendment mission of reconciling privacy and security. The point of asking whether the use of a particular surveillance technique is a “search” is to assess whether it leaves the opportunities for privacy and anonymity, in private and public space, essentially unscathed. If it does not, or if it undermines citizens’ confidence in the privacy-protecting features of their environment by eroding them or providing government with a detour around them, then a “reasonableness” inquiry is needed. The inquiry must determine, first, whether the damage done is justified by sufficiently weighty crime control or other concerns, and second, whether the damage is limited enough to be consistent with minimal conditions of privacy and anonymity in a free and open society. Thus, even if the Supreme Court had decided that the detection methods in *Place*⁴⁵¹ and *Jacobsen*⁴⁵² threatened privacy, and therefore counted as “searches,” it could still have decided they were “reasonable searches”—hence, constitutionally permissible—when they played an important role in detecting and thwarting criminal activity and were used under constraints that made use of such invasive techniques tolerable by sufficiently blunting the damage to the privacy interests of innocent citizens.

The current “reasonable expectations” test for what constitutes a “search” invites a muddling of these two Fourth Amendment inquiries.⁴⁵³ This is because, whether it is reasonable for a person to expect privacy in a given situation depends in part on whether significant security concerns

449. *Kyllo v. United States*, 533 U.S. 27, 38–39 (2001) (hypothesizing that in some situations the use of ordinarily limited thermal imaging technology could be a search because it might reveal intimate details of a person’s life).

450. Some chemical detection devices can tell investigators much more than whether someone is carrying explosives or drugs. As one manufacturer of a neutron scanning device noted, the technology is sophisticated enough to tell the difference between olive oil and motor oil. See Garber, *supra* note 272.

451. 462 U.S. at 707.

452. 466 U.S. at 123–24.

453. As Akhil Amar points out, “in the landmark *Katz* case, the Court, perhaps unconsciously, smuggled reasonableness into the very definition of the amendment’s trigger: the amendment comes into play whenever government action implicates a ‘reasonable expectation of privacy.’” AKHIL REED AMAR, *THE CONSTITUTION AND CRIMINAL PROCEDURE: FIRST PRINCIPLES* 9 (1997).

require dispensing with certain privacy protections.⁴⁵⁴ The confusing result of this muddling is that, even when investigators use high-powered technology to uncover information that can only be uncovered by puncturing or circumventing barriers that we rely upon to protect privacy, courts sometimes implausibly claim that these investigators have not engaged in any “searching.” Such logic may in many cases produce the right result. It may, for example, allow police to search a property or person that they have good reason to search. But even when such reasoning does produce the right result, Fourth Amendment values do not benefit in the long run when courts pretend that a justifiable sacrifice of privacy is no sacrifice at all—instead of carefully explaining the considerations that make this sacrifice justifiable and insisting on safeguards to minimize whatever damage to privacy results.

Another related contrast exists between this proposed method of defining a “search” and that which courts have adopted under *Katz*. Under the inquiry proposed here, the only time that courts should conclude that a surveillance method requires no sacrifice of privacy is either when the technology being used is inherently without risk for the privacy-protecting features of our environment or when firm limitations at work in the particular case eliminate any such risk. When a court is unsure how firm a limitation is, it might, of course, build such a limitation into its holding. This action in a sense was what the high courts of Alaska and Vermont did when approving of limited video surveillance in public. They indicated that while they were classifying a certain, very limited use of video surveillance as a “nonsearch,” the government could not assume that it would be free of Fourth Amendment constraint if it used suspicionless video surveillance, or especially, as the Vermont Supreme Court stressed, if it did so on a wide scale. If the method of surveillance in question is unconstrained by such limitations, and crosses the spatial and normative boundary lines that create spaces for private and anonymous action, it should be classified as a “search” regardless of other considerations.

V. “Reasonable” Warrantless Searches: Using Surveillance Technology Against Terrorism

A. *Judicial Balancing of Privacy and Security (and Reasonableness Requirements Beyond Balancing)*

Even where courts erect a legal barrier to protect core privacy interests, the Fourth Amendment does not make this barrier an impassable one. Barriers raised to protect privacy may be lowered somewhat in the interest of

454. For example, it is less reasonable to expect privacy at the entrance to an airport gate, where maximal privacy protections might hamper efforts to preserve the safety of hundreds of passengers, than it is to expect privacy in a phone booth.

security. As the text of the Fourth Amendment makes clear, it allows “searches” when they are not “unreasonable,” and even deeply intrusive searches can, in some circumstances, be reasonable. Intrusions into the body, for example, are permissible under certain circumstances.⁴⁵⁵ Normally, the test of reasonableness is the ability of the police or authorities to obtain a “warrant” by convincing a magistrate that “probable cause” exists to believe that a search of a particular person or place will yield evidence of a crime. Courts have also allowed police to dispense with the warrant process when faced with the possibility that a suspicious individual is carrying a weapon.⁴⁵⁶

But in recent years the courts have also found room for searches when authorities have no basis for individualized suspicion at all. And they have been most willing to create constitutional space for warrantless searches when the threat faced by the government was an elusive one, threatening tremendous loss of life. As Justice O’Connor noted, they have been willing to dispense with both the warrant and probable cause requirements where “even one undetected instance of wrongdoing could have injurious consequences for a great number of people.”⁴⁵⁷ The Supreme Court has stated that warrantless searches are justifiable, for example, to prevent train wrecks that cause “great human loss”⁴⁵⁸ or to address health epidemics.⁴⁵⁹ It has allowed warrantless searches at the national border, where security is a significant concern,⁴⁶⁰ in highly-regulated industries in which government agencies often need to ferret out hard-to-detect evidence of hazards that could have significant consequences for numerous people,⁴⁶¹ and in other environments, like drug-plagued schools, where it finds that extensive

455. See *Schmerber v. California*, 384 U.S. 757, 769–70 (1966) (finding that although a police-ordered extraction of blood was a search, it was a reasonable means of acquiring evidence under the circumstances).

456. See, e.g., *Terry v. Ohio*, 392 U.S. 1, 25–26 (1968) (explaining that a limited search for concealed weapons is permissible without a warrant).

457. *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 675 (1995) (O’Connor, J., dissenting).

458. *Skinner v. Ry. Labor Executives’ Ass’n*, 489 U.S. 602, 628 (1989).

459. *Camara v. Mun. Court*, 387 U.S. 523, 539 (1967) (noting that while “routine area inspections” do require a warrant, the law traditionally upholds warrantless searches when necessary to address the possible spread of disease or contamination).

460. See *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985) (“Routine searches of the persons and effects of entrants [at the border] are not subject to any requirements of reasonable suspicion, probable cause, or warrant”); *United States v. Ramsey*, 431 U.S. 606, 619 (1977) (“[T]he longstanding recognition that searches at our borders without probable cause and without a warrant are nonetheless ‘reasonable’ has a history as old as the Fourth Amendment itself.”).

461. See *New York v. Burger*, 482 U.S. 691, 703–04 (1987) (finding the warrantless inspection of a vehicle-dismantling business clearly within the “established exception to the warrant requirement for administrative inspections in ‘closely regulated’ businesses”); *Donovan v. Dewey*, 452 U.S. 594, 603–04, 606 (1981) (permitting warrantless searches of mines and quarries pursuant to a federal act targeted at controlling the notoriously hazardous conditions of those settings).

searches are needed to serve “special needs, beyond the normal need for law enforcement.”⁴⁶²

Courts have sometimes said that such “suspicionless searches” are only acceptable to serve an administrative goal, not to gather evidence for criminal proceedings. In striking down a warrantless drug testing scheme in *Ferguson v. City of Charleston*, for example, the Supreme Court noted that the involvement of the police in the testing scheme distinguished it from warrantless searches the Court had found permissible in the past, stating that it had “tolerated suspension of the Fourth Amendment’s warrant or probable-cause requirement in part because there was no law enforcement purpose behind the searches in those cases, and there was little, if any, entanglement with law enforcement.”⁴⁶³

In spite of this oft-stated rule limiting suspicionless searches to the administrative context, the Supreme Court has left little doubt that it would allow use of such searches to apprehend terrorists. Indeed, even as the Supreme Court forbade the use of suspicionless road block stops as a method of “ordinary crime control,” it noted that “the Fourth Amendment would almost certainly permit an appropriately tailored roadblock set up to thwart an imminent terrorist attack or to catch a dangerous criminal who is likely to flee by way of a particular route.”⁴⁶⁴ Even in the absence of any information that a terrorist attack is “imminent,” of course, courts have allowed ongoing suspicionless searches to detect weapons at airports⁴⁶⁵ and federal buildings.⁴⁶⁶ Although some courts have said that such programs are designed simply to protect the safety of air travelers,⁴⁶⁷ it seems disingenuous

462. *New Jersey v. T.L.O.*, 469 U.S. 325, 351 (1985) (Blackmun, J., concurring) (permitting the warrantless inspection, by an assistant vice principal, of a student suspected of having cigarettes at school); see also *Vernonia Sch. Dist.*, 515 U.S. at 646, 653 (quoting *T.L.O.*) (permitting the warrantless analysis of the urine of students participating in interscholastic athletics); *Skinner*, 489 U.S. at 619, 621–22 (quoting *T.L.O.*) (permitting under regulations promulgated by the Federal Railroad Administration the warrantless analysis of the urine of railroad employees following major train accidents); *Nat’l Treasury Employees Union v. Von Raab*, 489 U.S. 656, 677 (1989) (quoting *T.L.O.*) (permitting warrantless drug testing of Customs employees seeking promotion to positions that directly involve the interdiction of illegal drugs or that require carrying a firearm).

463. 532 U.S. 67, 79 (2001).

464. *City of Indianapolis v. Edmond*, 531 U.S. 32, 44 (2000).

465. *United States v. Edwards*, 498 F.2d 496, 500 (2d Cir. 1974); *United States v. Epperson*, 454 F.2d 769, 771 (4th Cir. 1972) (noting the “overwhelming government interest” in protecting air travelers from crimes that might “endange[r] the lives of thousands of people”); see also LAFAYE, *supra* note 52, § 10.6 (discussing suspicionless searches in airports).

466. See LAFAYE, *supra* note 52, § 10.7 (discussing suspicionless searches in federal buildings).

467. See *United States v. Davis*, 482 F.2d 893, 908, 910–11 (9th Cir. 1973) (stating that “[t]he essential purpose of the scheme is not to detect weapons or explosives or to apprehend those who carry them, but to deter persons carrying such material from seeking to board at all” and insisting that “airport screening searches are valid only if they recognize the right of a person to avoid search by electing not to board the aircraft”).

for anyone to argue that the point of such searches is simply to deter a would-be terrorist and not to apprehend and incapacitate him through the use of the criminal justice system.⁴⁶⁸

Ongoing suspicionless video surveillance may be defended on similar grounds, as an essential tool in the battle against terrorism. As terrorists have expanded their targets beyond airplanes, to buildings, hotels, and crowded plazas, law enforcement has had to similarly expand its reach. But this argument requires more than a simple adaptation of the Court's administrative search cases. In one crucial respect, the use of video surveillance on streets is strikingly different from warrantless searches in schools, workplaces, and airports. When courts have allowed suspicionless searches in the past, they have justified such searches by pointing not only to the important safety interest they were designed to serve, but also to the fact that such searches generally took place in environments where individuals' behavior was already subject to monitoring and regulation. The suspicionless drug testing allowed in *Skinner*, *Von Raab*, and *Vernonia School District*, for example, took place in schools and in federal employment contexts, environments where expectations of privacy are already reduced by rules of conduct and supervision arrangements necessary to such institutions.⁴⁶⁹ The additional testing required by the government was not a jarring and out-of-place intrusion, entirely unlike many of the other requirements already operating to limit the freedom of students and federal workers.⁴⁷⁰

468. For this reason, subsequent courts have rejected the Ninth Circuit's statement in *Davis* that an air traveler must be free to avoid a search by leaving an airport. As the Eleventh Circuit has stated, such a right to leave would constitute a "one-way street for the benefit of a party planning airport mischief, since there is no guarantee that if he were allowed to leave he might not return and be more successful." *United States v. Herzbrun*, 723 F.2d 773, 776 (11th Cir. 1984). Even the Ninth Circuit itself has reconsidered and limited *Davis*'s holding, allowing exit only before a passenger places his bags on an x-ray belt. *See United States v. Pulido-Baquerizo*, 800 F.2d 899, 902 (9th Cir. 1986) ("A rule allowing a passenger to leave without a search after an inconclusive x-ray scan would encourage airline terrorism by providing a secure exit where detection was threatened.").

469. *See Skinner v. Ry. Labor Executives' Ass'n*, 489 U.S. 602, 628 (1989) ("The covered employees have long been a principal focus of regulatory concern" because a train "becomes lethal when operated negligently by persons who are under the influence of alcohol or drugs."); *Nat'l Treasury Employees Union v. Von Raab*, 489 U.S. 656, 672 (1989) ("Unlike most private citizens or government employees in general, employees involved in drug interdiction reasonably should expect effective inquiry into their fitness and probity. Much the same is true of employees who are required to carry firearms."); *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 656 (1995) ("Fourth Amendment rights, no less than First and Fourteenth Amendment rights, are different in public schools than elsewhere; the 'reasonableness' inquiry cannot disregard the schools' custodial and tutelary responsibility for children.").

470. *See Von Raab*, 489 U.S. at 671 ("We have recognized . . . that the 'operational realities of the workplace' may render entirely reasonable certain work-related intrusions by supervisors and co-workers that might be viewed as unreasonable in other contexts.").

By contrast, the streets, parks, and public squares where public video surveillance takes place are in many ways the antithesis of monitored spaces. They are not tightly-regulated environments, where people have to answer regularly to supervisors or fit their behavior within the constraints of a particular regime aimed at serving particular purposes. On the contrary, as the Supreme Court has stressed in the context of the First Amendment, streets, parks, and public squares are places where individuals have heightened expectations of liberty.⁴⁷¹ They are in many ways the last refuge in society for open and untrammelled discussion. And, as the Supreme Court has acknowledged in its First Amendment “public forum” doctrine, they are places where individuals’ interest in free discourse often trumps many other important government interests. While those walking through a street or park are subject in such open areas to the casual observation of others, this does not mean that they are, or expect to be, subject to close and unrelenting monitoring.⁴⁷² As one federal court recently indicated, when one finds oneself under the close watch of government-operated video cameras, this is a strong sign that one is *not* in the kind of “public forum” traditionally found in streets, parks, and public squares.⁴⁷³

Because of their traditional function as enclaves of free and spontaneous thought and action, these public environments are ill-suited to absorb massive camera networks. Permitting pervasive state monitoring in these

471. See, e.g., *Hazelwood Sch. Dist. v. Kuhlmeier*, 484 U.S. 260, 267 (1988) (contrasting, in the First Amendment context, the significant liberty we expect in parks and streets to that which students can expect in the more controlled environment of a school).

472. Moreover, there is another reason that public and open spaces are particularly unsuitable places for such monitoring. As George Radwanski, the former Privacy Commissioner of Canada, has noted that when people are taped in banks and convenience stores there is an element of consent.

If you don’t want to appear before a camera, you have the choice of refusing to enter a given store. But if we end up with cameras all over our public streets, short of levitating above them, you have no way of withholding consent and still getting from place to place.

George Radwanski, *Privacy in Canada: Emerging Issues for Business and Society*, Address Before the Kelowna Chamber of Commerce (Feb. 6, 2002), at http://www.privcom.gc.ca/speech/02_05_a_020206_e.asp.

473. See *United States v. Demott*, 151 F. Supp. 2d 706, 711 (E.D. Va. 2001) (finding that the area just outside the entrance of the Pentagon was not a public forum, and pointing—in support of this finding—to the fact that “most of the grounds are constantly under surveillance by video cameras”). Even where the government wished to conduct much briefer suspicionless searches for drugs or bottles at rock concerts or shows in public arenas, courts have frequently held these searches unconstitutional, and have stressed that the threat of unruly behavior at such events is far different from the “unique circumstances” created by the threat of “airplane bombings” or “hijackings.” *Gaioni v. Folmar*, 460 F. Supp. 10, 13 (M.D. Ala. 1978); see also *Nakamoto v. Fain*, 635 P.2d 946, 951 (Haw. 1981) (holding that the city’s interest in safety at a rock concert did not justify the city’s requirement that each patron submit to a search before entering the public arena).

preserves of liberty is in some sense akin to allowing large-scale industrial production in what is supposed to be an unsullied nature sanctuary: whatever benefits, in safety or commerce, it may bring, it is both jarringly out of place and deeply damaging to the surrounding environment.⁴⁷⁴

How then are courts to react when asked to analyze the reasonableness of using pervasive video surveillance to counter a pervasive security threat? At a minimum, such a response would require a rethinking of the Court's suspicionless search analysis. But such a rethinking might proceed along a number of different lines.

First, one might take the position that because terrorists might cause deadly attacks anywhere, suspicionless searches have to be permissible anywhere. Such a stance appears to receive some support from polls suggesting that in the wake of September 11, 2001, Americans believe that once unacceptable sacrifices of privacy must now be made to meet once unimaginable threats to security.⁴⁷⁵ It is also in accord with the sentiments,

474. Even without the rethinking of Fourth Amendment jurisprudence proposed in this paper, courts should be especially wary of surveillance in public fora for the reasons the court has already given in *Zurcher v. Stanford Daily*: because "unrestricted power of search and seizure could also be an instrument for stifling liberty of expression," the Fourth Amendment must be applied with "scrupulous exactitude" where First Amendment interests are at stake. 436 U.S. 547, 564 (quoting *Marcus v. Search Warrant*, 367 U.S. 717, 729 (1961) and *Stanford v. Texas*, 379 U.S. 476, 485 (1965)). Such concerns should loom large in Fourth Amendment thinking not only when the government installs cameras on streets and parks, but also when it orders the installation of cameras in privately-run bookstores, libraries, or other sites that provide crucial support for anonymous exploration of ideas. Courts have defended such anonymous exploration of ideas against government attempts to investigate individuals' reading materials. See, e.g., *Tattered Cover, Inc. v. City of Thornton*, 44 P.3d 1044, 1052-53 (Colo. 2002). But when the threat to anonymous information-seeking comes not from officials' review of reading lists but from cameras installed to deter crime, it is not clear that courts applying the Fourth Amendment are likely to offer sufficient protection. Consider, for example, the recent case of *Vo v. City of Garden Grove*, 9 Cal. Rptr. 3d 257 (Ct. App. 2004). The court there upheld a city's requirement that CyberCafes install and operate video surveillance cameras inside their premises in order to deter and facilitate responses to criminal activity of the kind which had occurred in a few local CyberCafes. Analyzing this ordinance under the California constitution's privacy protections, the court refused to find that people have a reasonable expectation of privacy in their "activity on the premises or their physical features," *id.* at 276, and noted that there is already "near ubiquitous use of video surveillance in retail establishments, at automated bank teller machines, and at road intersections." *Id.* at 277. As the dissent points out, such an approach ignores the fact that "[C]ybercafes are *not* just ordinary retail establishments—they are the poor man's printing press and private library." *Id.* at 283 (Sills, J., dissenting). The court's answer—that "[t]he ordinance does not require video surveillance of e-mail or images from the Internet," *id.* at 275—paid no attention to whether cameras would nonetheless chill speech and receipt of information by capturing pictures of CyberCafe patrons that might later allow officials (or others) to link web site visits to particular individuals. Even if the city's crime problems justified additional safety protection in local CyberCafes, the question of what safety controls are reasonable should have been analyzed with special attention to the Supreme Court's statement in *Zurcher v. Stanford Daily*.

475. See, e.g., Gary Langer, *Terror vs. Liberties, Poll: Americans Believe Stopping Terror is More Important than Privacy*, ABCNEWS.COM (June 11, 2002) (giving the results of an

expressed by some, that the threat posed by terrorism and perhaps by other kinds of violent crime has already radically changed public life in a way that demands an equally radical change in the security protections offered by government.

People may welcome increased monitoring even when the threats they face in public do not produce mass casualties. The recent sniper attacks in Washington, D.C., for example, succeeded in shutting down a significant portion of public life for a period of weeks.⁴⁷⁶ In many crime-ridden neighborhoods in American cities, similar random violence is a feature of everyday life. People in such circumstances understandably may welcome surveillance techniques they would otherwise oppose to free themselves from the sense of being prisoners in their homes. Fourth Amendment protections might have to be adapted not only to new forms of government surveillance unimagined by the founders, as Brandeis stressed,⁴⁷⁷ but also to new forms of private violence that are more devastating than any forms of private violence known to the drafters of the Bill of Rights.⁴⁷⁸

At the core of such an argument is the assumption that no matter how intrusive the search, it can count as reasonable if the threat it is designed to meet is very grave. This stance appears to echo the Supreme Court's "proportionality" test, which holds that permissibility of a particular practice "is judged by balancing its intrusion on the individual's Fourth Amendment interests against its promotion of legitimate governmental interests."⁴⁷⁹ But this formulation of the proportionality test is too simple in that it fails to recognize constitutional democracies' need to preserve the minimal level of privacy and anonymity necessary to support individual autonomy. Such a reconciliation requires more than a weighing contest to determine which interest—safety or privacy—trumps the other in a specific instance. It requires measures designed to ensure that, even when certain powerful surveillance measures are desperately needed, they are used in a way which does not do irreparable damage to core principles of the constitutional

ABC/Washington Post poll, that found that a majority of Americans were in favor of giving the FBI greater authority to monitor public places even while acknowledging that such an expanded authority represented an intrusion on privacy rights), at http://abcnews.go.com/sections/us/DailyNews/terror_poll020610.html.

476. See Monte Reel, *A Region Running Scared?: Response May Be Excessive, But Situation is Unique, Experts Say*, WASH. POST, Oct. 19, 2002, at A1.

477. *Olmstead v. United States*, 277 U.S. 438, 472–73 (1928) (Brandeis, J., dissenting).

478. It is not only the appearance of novel, more devastating threats which makes people more willing to demand measures that better protect lives, but also a change in moral culture that has arguably led people to be less tolerant of events that lead to death or serious injury.

479. *Skinner v. Ry. Labor Executives' Ass'n*, 489 U.S. 602, 619 (1989) (quoting *Delaware v. Prouse*, 440 U.S. 648, 654 (1978)).

order.⁴⁸⁰ Moreover, the simplest formulation of the Court's balancing test fails to register that measures which eliminate privacy protections are intuitively more disturbing, and harder to see as reasonable under any conditions, than the more familiar measures of ensuring Fourth Amendment "reasonableness," which suspend or temporarily circumvent such privacy protections. Warrants authorize home entries, but walls continue to conceal private activities after such a search is conducted, and while drug tests uncover medical information, one's medical and biological condition does not indefinitely remain open to examination. By contrast, camera networks that unalterably change citizens' public spaces may cause permanent damage to their freedom from monitoring.

How then can courts protect core Fourth Amendment privacy interests while allowing the government sufficient room to battle terrorism? Apart from simply asking whether a particular security measure is reasonable, there are three categories of safeguards—two of which have been considered in past cases⁴⁸¹—that courts might insist upon in Fourth Amendment cases to make sure that technologically-enhanced searches remain safe for constitutional democracy. First, they can ask law enforcement to respect the kinds of constraints that courts have treated as "warrant substitutes" or "warrant equivalents" even when circumstances do not permit, or justify, requiring review by a neutral magistrate. These include making sure a particular search regime has built-in limitations which confine investigators to a narrow purpose or to a well-defined and difficult-to-abuse set of procedures. Second, they might selectively introduce warrants into parts of a warrantless search process that presents a particularly significant threat to privacy and can await review by a neutral magistrate. For example, even if the police cannot wait for magistrate review to begin observing a certain activity on video, courts might ask them to get a warrant before using that

480. The former Privacy Commissioner of Canada has provided a helpful illustration of why there is a certain price that a civilized society cannot pay even when it is desperate for additional security: "[W]e could be safer from terrorism if we permanently evacuated . . . high-rise office towers," "closed down the underground," or "grounded all airplanes." George Radwanski, Speech at the London School of Economics (Sept. 6, 2002), available at http://www.privcom.gc.ca/media/nr-c/02_05_b_020906_e.asp; see also Blair: Don't Do Terrorists' Job for Them, CNN.COM, Nov. 12, 2002 (reporting a speech by Prime Minister Blair emphasizing that the government could not shut down every site threatened by terrorists), available at <http://www.cnn.com/2002/world/europe/11/11/uk.blair.warning/index.html>. But such measures—although perhaps the only way to reduce certain security risks to zero—are inconsistent with retaining the core elements of a modern constitutional democracy. The features of public environments that allow us to move freely and with a high degree of anonymity are of course more intangible than urban structures or transportation centers, but eliminating them (as ubiquitous cameras might one day do) would alter the fabric of day-to-day life and constrain individual opportunities just as significantly.

481. For a discussion of the safeguards applied by courts in the past, see *infra* sections V(A)(1)–(2).

video to track or magnify a particular individual or using facial recognition to identify him. Both of these approaches have received some attention from judges and legislators. There is a third approach which is more unfamiliar to contemporary Fourth Amendment caselaw. It involves allowing wide-scale warrantless and suspicionless *unmonitored* recording, but stringently controlling any human review of such recording (either by requiring warrants or warrant equivalents). These three approaches are not mutually exclusive. Rather, each of them is a separate “tool set” of sorts that courts might use in their Fourth Amendment reasonableness analyses to ensure that core protections for privacy survive even in the midst of pressing security needs. To better explain how they can do this, I briefly examine each of these three possibilities below.

1. *Warrant Substitutes and Minimization.*—Even in suspicionless searches where a warrant or probable cause requirement cannot exist without destroying the effectiveness of the search, courts can and should demand “a constitutionally adequate substitute for a warrant.”⁴⁸² Even in such suspicionless searches, there is some constitutionally-mandated requirement or set of requirements that serves the key functions of a warrant, which are to “assur[e] citizens subject to a search or seizure that such intrusions are not the random or arbitrary acts of government agents” and that “the intrusion is authorized by law, and that it is narrowly limited in its objectives and scope.”⁴⁸³ Notably, courts do not suggest that the need for such a “warrant equivalent” disappears in the face of a significant security risk. On the contrary, there is an expectation that even when a warrant is impracticable, a warrant equivalent is generally required.

In earlier cases, courts have found adequate constraints in a number of factors. Specifically, the warrantless searches that courts have allowed are often constrained in three ways:

(I) They leave the searching official with little discretion because of the standardization in:

- (a) the purposes for which the search will be administered;⁴⁸⁴
- (b) how the search is conducted;⁴⁸⁵ and

482. See, e.g., *New York v. Burger*, 482 U.S. 691, 703 (1987); *Donovan v. Dewey*, 452 U.S. 594, 603 (1981).

483. *Skinner*, 489 U.S. at 621–22 (upholding regulations promulgated by the Federal Railroad Administration that authorize the warrantless analysis of the urine of railroad employees following major accidents).

484. See, e.g., *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 658 (1995) (noting that “it is significant that the tests at issue here look only for drugs, and not for whether the student is, for example, epileptic, pregnant, or diabetic”).

(c) the population on whom the search will be administered.⁴⁸⁶

(2) They are relatively nonintrusive in that they:

(a) are brief—and often only operate as an “entry condition” rather than an ongoing monitoring system;⁴⁸⁷

(b) are often entirely avoidable;⁴⁸⁸

(c) reveal little information—often only the presence or absence of drugs or metallic objects;⁴⁸⁹ and

(d) occur against the backdrop of regulated environments—leaving freer environments relatively untouched.⁴⁹⁰

(3) The necessity of the search is clear even without a review by a neutral magistrate because:

(a) the evidence available to those who created the search regime made it clear that the security problem it targets is a serious one;⁴⁹¹ and

(b) the type of search used is well-suited to address this problem.⁴⁹²

Not all of these limitations are feasible in the context of public video surveillance in public streets. Unlike searches in schools or workplaces, the

485. See, e.g., *id.* at 658 (noting that “the drugs for which the samples are screened are standard, and do not vary according to the identity of the student”).

486. See, e.g., *Nat’l Treasury Employees Union v. Von Raab*, 489 U.S. 656, 667 (1989) (“The process becomes automatic when the employee elects to apply for, and thereafter pursue, a covered position. . . . [T]he Service does not make a discretionary determination to search based on a judgment that certain conditions are present . . .”).

487. See, e.g., *id.* at 664 (upholding drug testing as an initial condition for employment in positions involving drug interdiction or the handling of firearms).

488. See, e.g., *Vernonia Sch. Dist.*, 515 U.S. at 657 (“By choosing to ‘go out for the team,’ [student athletes] voluntarily subject themselves to a degree of regulation even higher than that imposed on students generally.”); *Von Raab*, 489 U.S. at 667 (noting that “every employee who seeks a transfer to a covered position knows that he must take a drug test”); *United States v. Davis*, 482 F.2d 893, 910–11 (9th Cir. 1973) (observing that it is necessary that one be able to “avoid [the] search by electing not to board the aircraft”).

489. See, e.g., *Von Raab*, 489 U.S. at 672 n.2 (“[U]rine samples may be examined only for the specified drugs. The use of samples to test for any other substances is prohibited.”).

490. See, e.g., *United States v. Taketa*, 923 F.2d 665, 673 (9th Cir. 1991) (explaining that certain employees have a diminished expectation of privacy because of the “operational realities” of the workplace).

491. See, e.g., *Vernonia Sch. Dist.*, 515 U.S. at 661 (noting the importance of “[d]eterring drug use by our Nation’s schoolchildren”).

492. See, e.g., *City of Indianapolis v. Edmond*, 531 U.S. 32, 42–43 (2000) (declaring that “the gravity of the threat alone cannot be dispositive of questions concerning what means law enforcement officers may employ to pursue a given purpose. Rather, in determining whether individualized suspicion is required, we must consider the nature of the interests threatened and their connection to the particular law enforcement practices at issue”).

effects of searches in streets or parks are not limited to regulated environments, leaving freer environments undamaged. Nor does it seem possible to make the cameras entirely avoidable; on the contrary, doing so might defeat their purpose by giving would-be criminals a means of eluding them.

However, governments can make public cameras less privacy-invasive by imposing some of the constraints listed above. Perhaps the most obvious step they might take is to significantly limit the purposes for which video surveillance may be used. One version of such a purpose limitation is set out in the ABA Standards for Physically-Assisted Physical Surveillance, which requires that police use public video surveillance only when doing so is “reasonably likely to achieve a legitimate law enforcement objective.”⁴⁹³

This standard puts some valuable limits on use of powerful new surveillance technologies. Police, for example, could not build profiles of hundreds of law abiding citizens simply on a hunch that such profiles might one day prove useful in solving a crime. But the ABA’s limitation is still too broad. Authorizing the use of video surveillance for any law enforcement purpose allows officials to take video cameras, reluctantly accepted as tools for fighting violent criminals, and turn them on suspected shoplifters or petty thieves. As Jeffrey Rosen observes, such a transformation is precisely what occurred in Great Britain when public cameras proved to be of little help in fighting terrorism.⁴⁹⁴ While use of video surveillance to solve relatively minor, nonviolent crimes does benefit society (for example, in the form of less theft), it also carries a significant cost for anonymity and privacy in public life. As Michael Adler has noted in discussing electronic computer searches, such interest in nonviolent crimes brings pervasive police scrutiny closer to the realm of ordinary citizens’ day-to-day lives.⁴⁹⁵ Camera operators charged with stopping shoplifters or pickpockets will have reason to closely scrutinize more ordinary activity than operators charged only with looking for evidence of violent crimes.

Moreover, stricter limitations on purpose have strong support in federal court precedent. In *City of Indianapolis v. Edmond*, the Supreme Court forbade the use of roadblocks for “ordinary crime control” and complained that a standard allowing roadblocks in this way would provide “little check on the authorities’ ability to construct roadblocks for almost any conceivable law enforcement purpose.” If this were permitted, said the Court, “the Fourth Amendment would do little to prevent such intrusions from becoming

493. See ABA STANDARDS OF CRIMINAL JUSTICE, *supra* note 147, Standard 2-9.3, at 69.

494. Rosen, *supra* note 11, at 41–42.

495. See Adler, *supra* note 288, at 1110 (discussing how electronic computer searches could influence a person’s actions in the privacy of his home).

a routine part of American life.”⁴⁹⁶ To guard against this possibility, the Court insisted that warrantless road block examinations could be used only for certain “programmatically purposes” for which such a device is suited, especially purposes related to road safety. Although warrantless roadblocks might prove useful in turning up evidence of just about any crime—police might find evidence of narcotics, guns, counterfeiting, just about anything someone could carry in a car—this was not an excuse for forcing all drivers on the road to submit to random searches.⁴⁹⁷

Other courts have raised similar concerns about searches for weapons at airports. In *United States v. Albarado*, for example, the Second Circuit worried that “there is the possibility that the purpose of the airport search may degenerate from the original search for weapons to a general search for contraband.”⁴⁹⁸ In *United States v. Davis*, the Ninth Circuit likewise took note of the “obvious danger . . . that the screening of passengers and their carry-on luggage for weapons and explosives will be subverted into a general search for evidence of crime.”⁴⁹⁹ The Ninth Circuit acted to stave off such a danger in a later case, where it struck down a regime which rewarded airport screeners for ferreting out evidence of all kinds of criminal wrongdoing beyond threats to air safety.⁵⁰⁰ The Ninth Circuit acknowledged that “the contents of billions of satchels, purses, briefcases and pockets will naturally strain out much that is of interest to law enforcement,” but stressed that this did not justify converting limited airport security into unlimited warrantless

496. 531 U.S. 32, 42 (2000).

497. The Supreme Court’s recent decision in *Illinois v. Lidster*, 124 S. Ct. 885 (2004), does not appear to limit *Edmond*’s restriction on police use of roadblock searches. In *Lidster*, the Supreme Court upheld police use of a checkpoint to ask motorists if they had any information about a fatal hit-and-run accident that had occurred near the checkpoint in the previous week. As the Court made clear, the checkpoint was acceptable because it was akin to the sort of voluntary questioning that police conduct when they seek help from pedestrians. *Id.* at 890. Unlike the roadblock in *Edmond*, the checkpoint at issue in *Lidster* did not involve any search of the motorist at all, for its purpose “was *not* to determine whether a vehicle’s occupants were committing a crime, but to ask vehicle occupants, as members of the public, for their help in providing information about a crime in all likelihood committed by others.” *Id.* at 889. *Lidster* does raise some doubt about the fear expressed in *Edmond* that roadblocks could become a “routine part of American life,” 531 U.S. at 42, if left free from strict constitutional limits: “limited police resources” and “community hostility to related traffic tie-ups,” writes Justice Breyer, should provide an effective check on excessive use of roadblocks, *Lidster*, 124 S. Ct. at 890. But regardless of how the Court assesses the danger of roadblock proliferation, Justice Breyer’s arguments seem unlikely to apply to video surveillance, which does not slow citizens’ movements and which many argue will cost less than current methods of crime control (particularly as cameras become cheaper and more powerful).

498. 495 F.2d 799, 805 (2d Cir. 1974).

499. 482 F.2d 893, 909 (9th Cir. 1973). Both the Second and Ninth Circuits noted with some concern that searches justified to protect air travelers’ safety were already being routinely used to discover drugs. *Albarado*, 495 F.2d at 805; *Davis*, 482 F.2d at 909.

500. *United States v. \$124,570 U.S. Currency*, 873 F.2d 1240, 1247–48 (9th Cir. 1989).

searches of everyone who has a need to travel.⁵⁰¹ Such a serious-crime limitation seems even more important when the surveillance technique in question can pierce peoples' privacy not simply as they prepare to board a plane, but anywhere in public space.⁵⁰²

Apart from limiting the purposes to which public camera systems are put, courts can also ensure that even when cameras are being used to counter serious crime, they are focused as narrowly as possible on achieving that purpose. Just as the existing legal regime for wiretap demands that police avoid, wherever possible, capturing details of innocent conversations,⁵⁰³ a legal regime for video surveillance might require that governments take reasonable measures to keep innocent, law-abiding activities off of government video screens. As Christopher Slobogin has observed, perhaps the most important measure of this kind is a strict limitation on suspicionless tracking of individuals.⁵⁰⁴ It is here, in a determination of a search technique's reasonableness, that the "minimization" requirement explored earlier is most useful. Cameras should not be locked onto particular people merely because government officials are interested in observing them, nor should officials be able to easily retrace someone's movements on camera footage without adequate grounds for doing so. As the Ninth Circuit stressed in *Taketa*, video searches are most offensive to Fourth Amendment values when they are "directed straight at" a person and are not simply searches of a place he happens to be.⁵⁰⁵

There are a number of measures government might take to ensure that cameras are not easily used to track or spy upon individuals. First, cameras might be trained on places or events instead of specific people. The police might point them only at areas, like subway platforms, where there is concern about crime, or at events, like large rallies, where there is a need for heightened security or crowd control. As Slobogin suggests, neighborhood-wide camera systems might be used only in areas where crime is a significant problem.⁵⁰⁶ Likewise, cameras might be activated only at specific times, such as when a terrorist alert requires heightened scrutiny in particular parts of a city. Moreover, even where spaces seem to require monitoring, courts might still ask whether camera systems can make public spaces sufficiently

501. *Id.* at 1246–47.

502. William Stuntz has proposed such a restriction for covert surveillance, and mentioned video surveillance as an example. He argues that "where the search tactic is both secret and potentially invasive, it should probably be limited to the investigation of violent felonies. The best way to ensure that result is to bar the use of such evidence to prove other, lesser crimes." Stuntz, *supra* note 61, at 2184.

503. 18 U.S.C. § 2518(5) (West 2000 & Supp. 2003).

504. Slobogin, *supra* note 38, at 295–96.

505. *United States v. Taketa*, 923 F.2d 665, 677 (9th Cir. 1991).

506. Slobogin, *supra* note 38, at 287–95.

safe by monitoring people only at certain “entry-points” to various spaces, instead of subjecting them to pervasive observation when inside.

Second, cameras and recording devices might track suspicious *activities or objects* instead of particular people, with the aid of pattern recognition software designed to identify guns or other weapons. Even if currently available pattern-recognition software does not allow for visual identification of bombs or other dangerous devices, one might ask whether video networks can be used in conjunction with, and activated by, other technologies that detect the chemical or magnetic “signatures” of such devices.⁵⁰⁷

Indeed, courts should ask not only whether such powerful technologies might be used in conjunction with video surveillance, but also whether they might be used *instead* of video surveillance. In a world where investigators might soon be able to use “smart dust” to detect chemical and biological weapons, and numerous other devices to detect “chemical signatures” of explosives and “magnetic signatures” of firearms,⁵⁰⁸ courts should ask what the less discriminating surveillance of public camera networks would add to these focused methods of detecting crime and terror threats, and whether the added benefit supplied by video surveillance is worth the loss of privacy it entails. Of course, courts are not well-equipped to judge which novel technologies are most likely to work. However, they can and should ask the government to address questions raised by defendants, or by amici curiae, about why particular alternative methods cannot provide the same security benefits with significantly less damage to privacy. Deliberation and debate about such issues might also occur in other forums for discussing the constitutionality of alternative security protection measures, such as in legislative debates about the constitutional limits on a legislative framework for use of new technologies by law enforcement.

Such inquiry is especially justified in light of the questionable track record of existing video surveillance and face recognition systems. A recent “meta-study” canvassed twenty-two empirical studies on existing video surveillance systems and reported that the results showed an ambiguous effect on crime.⁵⁰⁹ The aggregate reduction in crime, according to the meta-study, was only four percent.⁵¹⁰ And half of the studies found that the CCTV systems they examined had either no discernible effect on crime or an

507. One model for this kind of limitation—and how it can be used in conjunction with place limitations—is provided by *State v. Costin*, 720 A.2d 866, 869 (Vt. 1998). The video camera in that case was pointed at what police had already identified as a marijuana garden and was equipped with infrared sensors that initiated recording only when someone approached the garden. *Id.* at 867.

508. *See supra* subpart II(C).

509. BRANDON C. WELSH & DAVID P. FARRINGTON, CRIME PREVENTION EFFECTS OF CLOSED CIRCUIT TELEVISION: A SYSTEMATIC REVIEW 41–42 (Home Office Research Study 252, Aug. 2002), available at <http://www.homeoffice.gov.uk/rds/pdfs2/hors252.pdf>.

510. *Id.* at 41.

undesirable effect on crime.⁵¹¹ The reduction in crime was even more negligible—only two percent—in downtown areas, where many cities are placing cameras.⁵¹²

Such research, to be sure, does not justify the conclusion that video surveillance can never be an effective tool in the fight against violent crime or terror. Just as developing technology can make infrared detectors and camera systems of the future more threatening to privacy than those which exist now, the same technology—more powerful zoom lenses, more effective biometric identification technology—can make such infrared detectors and camera systems more effective in solving crimes or uncovering criminal enterprises. Moreover, law enforcement officials might find it difficult to demonstrate that a specific surveillance technology is successful in meeting the threat of terrorism unless they have a chance to experiment with different technologies to determine what works. Even promising technologies will not necessarily yield immediate benefits. However, such experiments might have significant costs for liberty and privacy. Therefore, a sound Fourth Amendment jurisprudence has to ensure that all technological experiments occur within constitutional boundary lines. Courts can tolerate, and even endorse, experimentation without unquestioningly endorsing surveillance systems that have no clear relation to the problem they are claiming to address, or seem like a superfluous addition to other, less invasive techniques for addressing the same problem.

Even when video surveillance does seem necessary, courts might insist on the sorts of minimization measures described above to thwart the more Orwellian uses of video surveillance.⁵¹³ Cameras that remain focused on one place are unlikely to follow individuals as they move through public space, creating a moment-by-moment record of their lives. Cameras that activate only in reaction to a reliable danger signal are unlikely to capture people as they read, converse, or stare through a shop window. Such limitations do not eliminate all cause for concern. Even a place-centered camera system might be quite intrusive if it covers many public places, including spaces like a city's libraries or public squares, which constitute natural sites for individuals to engage in spontaneous action or anonymously seek out alternatives to their existing way of life. If it is extensive enough, a set of video records that is originally created to provide a record of events in particular sites can provide the government with the raw material it needs to compile a record of many

511. *Id.* at 46; see also NIETO ET AL., *supra* note 20, at 13 (noting that “[d]espite their increasing use, there is limited evidence that CCTV camera surveillance programs are successful crime prevention tools”).

512. *Id.* Jeffrey Rosen notes that in 2001, “Britain’s violent crime rates actually increased by 4.3 percent, even though the cameras continued to proliferate.” Rosen, *supra* note 11, at 92.

513. See *supra* text accompanying notes 503–05.

citizens' movements and interests. And limiting camera systems to the taping of unlawful activity will hardly be limiting them at all if such systems are activated to track even those minor deviations from the law that are common and widespread. Individuals will hardly feel insulated against regular government observation in a world where officials regularly cast a "wide video net" for evidence of minor crimes, and thereby predictably haul in and review numerous visual records of ordinary activity. Minimization criteria must therefore be applied in a way that gives them force. While courts might, in an age of mass terrorism, accept the necessity of some systematic monitoring of public activities by government, they might at least insist on a system that cuts as little as possible into individual privacy and preserves for individual citizens a great, unmonitored realm of public space.

2. *Selective Warrants*.—Apart from employing general time, space, and purpose constraints of the sort they have used in other "warrantless search" cases,⁵¹⁴ courts might also resort to a more traditional means of limiting video surveillance: the warrant requirement itself. Of course, when government insists on the necessity of regularly keeping watch over subways and other public spaces, it may not be practical to require that it seek a warrant each time it does so. But courts might find a place for a warrant in a surveillance process by addressing such a process piece-by-piece. Even when use of a video camera is permissible without a warrant, use of zoom lenses to scrutinize someone or use of facial recognition technology to identify them might not be. Indeed, the District of Columbia City Council, the Virginia Legislature, and the California Legislature have all considered precisely such a "selective warrant" scheme, although Virginia and California ultimately opted not to adopt it.

Such a scheme helps answer one of the central concerns about placing Fourth Amendment limits on video surveillance. As the Supreme Court noted in *Ciraolo*, one of the reasons for rejecting substantial restrictions of the police's ability to make observations in public space is that the government needs some space where it can freely gather the information that it needs to justify the more intensive type of search that is possible only with a warrant.⁵¹⁵ Allowing for warrantless observation with *basic* video camera technology might give it such space and give it enough opportunity to collect the information it needs to decide for itself (and to allow a neutral magistrate to decide) whether magnification, biometric technology, or later viewing of recorded footage is necessary to engage in a more focused searching of particular places or individuals.

514. For a discussion of "warrantless search" cases, see *infra* subsection V(A)(1).

515. See *California v. Ciraolo*, 476 U.S. 207, 213 (1986).

Such a proposal also puts significant constraints on the most privacy-damaging aspects of modern video surveillance. As I noted earlier, the greatest threats posed by video surveillance result not simply from the government's pointing a camera at public space, as various cities have experimented with doing since the 1960s, but from recent technological developments allowing camera operators to establish links between multiple cameras and to store, search, or closely scrutinize images captured by these cameras.⁵¹⁶ It is not merely the use of video cameras, but substantial recording of images, and searching of stored images, for example, which threatens to transform our spontaneous behavior in public places into permanent, and possibly misleading, records for which we will be accountable. It is linking between cameras—as well as new tracking and biometric technologies—that allows governments to reconstruct people's activities and retrace their movements through a given day. And it is magnification and biometric technologies that allow camera operators to closely scrutinize or identify people whose identity and detailed behavior is otherwise likely to remain unknown.

Perhaps for these reasons, at least three state and local legislative bodies have already proposed selective use of warrants or court orders. The D.C. Council has recently proposed legislation that permits warrantless use of video surveillance for various law enforcement, security, and traffic purposes,⁵¹⁷ but requires a court order for any use of video surveillance with audio and of cameras that have “telescopic zoom capability” enabling “facial identification.”⁵¹⁸ Its restrictions on use of biometric technologies are even more stringent. The Act provides that “[t]he Mayor shall not use biometric technology or software in combination with any government use of video surveillance without specific legislative authorization.”⁵¹⁹ The proposed D.C. Act also generally allows videotape recording only when the police apply for and receive a court order, and only if the U.S. Attorney first authorizes such an application in writing.⁵²⁰

In a similar vein, members of legislatures in two states, Virginia and California, have considered requiring warrants for police use of facial

516. *See supra* subpart II(A).

517. *See* [Proposed] Limited Authorization of Video Surveillance and Privacy Protection Act of 2002, § 3, *available at* <http://www.dccouncil.washington.dc.us/images/00001/20030113171053.pdf> (last visited Apr. 9, 2004). Most uses of public cameras are for limited time periods: “[t]emporary management of public resources during major events,” “[t]emporary management of the flow of traffic . . . during times of heightened traffic congestion,” “[t]emporary use as part of an effort to prevent, detect, and investigate crime in neighborhoods pursuant to [a pilot project authorized elsewhere in the Act].” *Id.*

518. *Id.* § 6(a), (c).

519. *Id.* § 13(c).

520. *Id.* § 7.

recognition technology. The California bill, S.B. 169, would have required authorities to acquire a warrant prior to any government use of facial recognition systems,⁵²¹ but this warrant requirement was ultimately eliminated from the bill.⁵²² Virginia had a similar experience. The Virginia House passed, but a Virginia Senate panel subsequently rejected, warrant requirements for facial recognition designed to assure that it was used only when necessary and only for certain limited purposes.⁵²³ As a precondition for obtaining a warrant, the law would have required the Attorney General not only to describe the place where the technology was to be used, but also to provide reasons to think this place would attract criminal or terrorist activity, and to identify the persons or class of persons being sought.⁵²⁴ The bill would also have allowed use of facial recognition technology only to locate missing persons, persons with “outstanding felony warrants,” “persons or class of persons who are identifiable as affiliated with a terrorist organization,” and others whose match could provide “evidence of the commission of a felony or Class 1 misdemeanor.”⁵²⁵ This restriction puts limits on the purposes for which the technology can be used. Even if the pervasiveness or constancy of a terrorist threat weakens the time and space limitations on use of facial recognition technology, legislatures might still insist—as this proposed Virginia Bill required—that police have good grounds to think that a particular individual is associated with crime or terrorism before including that person in a face recognition database.⁵²⁶ Some might argue that such a requirement would undercut governments’ efforts to locate suspected terrorists with no criminal record.⁵²⁷ But such a criticism has little force when courts accept reliable intelligence information about terror connections as adequate grounds for entering someone’s face print into a facial recognition database.

521. S.B. 169, 2001 Leg., 2001–2002 Sess. (Ca.) (amended July 5, 2001), available at http://www.ibia.org/sb_169_bill_20010705_amended_asm.pdf.pdf.

522. *Id.* For a general discussion of S.B. 169, see David McCormack, Note, *Can Corporate America Secure Our Nation?: An Analysis of the Identix Framework for the Regulation and Use of Facial Recognition Technology*, 9 B.U. J. SCI. & TECH. L. 128, 144–45, 150–51 (2003).

523. H.B. 2506, 2003 Gen. Assem., Reg. Sess. (Va. 2003).

524. *Id.* § 19.2-70.6(A)(2).

525. *Id.* § 19.2-70.5(B).

526. See McCormack, *supra* note 522, at 150 (noting that “[i]nstead of requiring a warrant for the use of facial recognition technology, Congress should require that law enforcement could only include an individual in the database pursuant to a warrant”).

527. See, e.g., Letter from William W. Wilson, Chairman, International Biometric Industry Association, to Honorable Darrell Steinberg, Chairman, California Assembly Judiciary Committee, para. 8 (June 18, 2001) (“If an associate of Usama Bin Laden is known to be targeting the crowd at Los Angeles International Airport for a terrorist attack, SB 169 would require the Los Angeles Police Department to obtain a warrant before facial recognition technology could be used to simplify the search.”), available at <http://www.ibia.org/newslett010606.htm>.

The above initiatives came from legislatures. But courts should insist on similar requirements as a constitutional matter. Even when a state or locality is unwilling to protect the character of its public space, this does not mean that individuals within that state or locality should therefore be without safeguards against intrusive video monitoring that undercuts core Fourth Amendment interests. Courts should not necessarily require a warrant in all circumstances when a locality wishes to use recording or facial recognition. In some cases, what I have called “warrant equivalents” might be more appropriate, and participants in the recent debate over video surveillance in D.C. have recognized that communities should have significant input into determining the necessity and scope of any camera network placed over their streets.⁵²⁸ But courts might insist that, regardless of the preferences of a community and its elected representatives, any video or other technology-assisted surveillance must meet certain minimal conditions designed to limit the damage such surveillance can cause to the privacy-protecting features of public space.

3. *Unmonitored Recording and Carefully-Restricted Viewing*

a. The Advantages of Automatic Video Cameras.—There is also a third broad approach to making video surveillance less privacy-invasive. The essence of this approach can be summarized as follows: unmonitored cameras should record everything, so that government investigators see nothing, except the minimum they need to see in order to serve the narrow mission they are charged with serving. Such a system emulates the legal regime for past-tracing in the world that Lewis Padgett describes in his story, “Private Eye,” where recordings are made automatically, but then reviewed by no one except on the basis of probable cause.⁵²⁹

To be sure, in Padgett’s fictional world, this automatic recording is not really an option; it is an unalterable part of the machinery of the physical universe. While privacy-conscious citizens and courts can use the legal system to keep the government from watching individual histories, the laws of nature operating in Padgett’s imagined society condemn its inhabitants to

528. See Constitution Project Comments to the City Council of the District of Columbia on the “Limited Authorization of Video Surveillance and Privacy Protection Act of 2002,” App. A, at 4 (noting that the D.C. police department should “discuss publicly with targeted communities the placement of cameras” and that the department had stressed that “there ‘would have to be widespread community support for the use of the technology’ prior to its deployment in residential neighborhoods”), available at [http://www.constitutionproject.org/lc/DC_Council_comments_on_Patterson_Bill_\(12-10\)2.doc](http://www.constitutionproject.org/lc/DC_Council_comments_on_Patterson_Bill_(12-10)2.doc) (last visited Mar. 21, 2004); see also Slobogin, *supra* note 38, at 286 (arguing that the “judicial objective should be merely to establish the regulatory framework; law enforcement agencies and the political process can fill in the details”).

529. See *supra* text accompanying notes 1–10.

live in a world that automatically records these histories. In other words, the legal system does not control the recording of visual records; it only controls access to them.

We, of course, have a choice unavailable to the inhabitants of Padgett's world. Where it is artificial, human-operated cameras that do the recording, the legal system might control not only whether and when investigators have access to visual records of our past, but whether (and under what circumstances) such records are created in the first place, and how they are to be maintained while in existence, and destroyed when there is no need for them. Many commentators might argue that we should exercise this choice to avoid unmonitored recording at all costs. Even when records of our lives are strictly controlled, recording of our public activities still makes us more vulnerable to systematic scrutiny, and might well chill spontaneous activity or behavior that is unconventional (but legal and nonharmful). As Michael Froomkin points out, "[a] data subject has significantly less control over personal data once information is in a database" and "[t]he easiest way to control databases, therefore, is to keep information to oneself: If information never gets collected in the first place, database issues need never arise."⁵³⁰ Moreover, regimes for protecting recorded data can change. Controls that exist one day can cease to exist the next. Thus, even if we are victorious in keeping our pasts from being viewed in a screening room, if our past is captured in video records, this victory may only be a temporary one, because the records of our lives might be viewed another day.

The above problems characterize all recording of our lives, whether by human beings or unmonitored machines. But some commentators have stressed that unmonitored recording by machines is especially problematic, because most machines cannot, at least in this day and age, reliably distinguish suspicious from innocent activity.⁵³¹ As James Carr and Patricia Bellia have noted in the contexts of communications interception, "[p]articuliarization of the conversation to be overheard, and the related statutory requirement that the surveillance be minimized cannot be accomplished in the context of unmonitored recording" and thus it is hard to see how such recording could comply with the Fourth Amendment.⁵³²

530. A. Michael Froomkin, *The Death of Privacy*, 52 STAN. L. REV. 1461, 1464 (2000).

531. Wiretap devices might conceivably be triggered by certain words, and video recorders, like the one in *State v. Costin*, 720 A.2d 866 (Vt. 1998), might conceivably be triggered by suspicious objects or approaching suspicious places, but while such limited recording might be useful in particular situations, it could probably be easily evaded by a change of code words or strategies. Also, there may be circumstances where police will not know what they are looking for until after the fact.

532. JAMES G. CARR & PATRICIA L. BELLIA, *THE LAW OF ELECTRONIC SURVEILLANCE*, § 3.2(e)(1)(A), at 3–36 (2002).

However, for a number of reasons, courts should at least take such unmonitored recording seriously as a possible tool for minimizing the harm done by video surveillance. First, unlike monitored recording, the activities captured by unmonitored recording might never be seen by anyone. Visual records might be created, unobserved by anyone, locked in a machine, and then automatically destroyed after a set period of time, except when a serious crime in a certain area, or closely connected with a certain area, gives police good reason to keep and view relevant recordings. Such a system may leave people less self-conscious about engaging in spontaneous activity in public places, because in most circumstances, they will be able to retain the sense that they are free from having a constant audience. As Daniel Solove writes, “[b]eing observed by an insect on the wall is not invasive for privacy; rather, privacy is threatened by being subject to *human* observation, which involves judgments that can affect one’s life and reputation.”⁵³³

Second, such a system may also help satisfy one of the key purposes of a “constitutionally adequate substitute for a warrant,” which is to control the discretion of officials.⁵³⁴ There may be great benefits to removing human control from the part of the video surveillance process where discretion may be most difficult to eliminate: namely, decisions about what to record. As Andrew Senior and Ruud Bolle point out, especially when supplemented with “[a]utomatic identity masking controls,” facial recognition technologies may be less privacy-intrusive than human visual surveillance systems because an automatic surveillance system can allow access to video only when a security incident has been detected.⁵³⁵ Once visual data is in a database, it may be easier to subject its analysis to a set of rules that help prevent the viewing of activities unrelated to crime,⁵³⁶ especially after police have gathered additional information that might help focus what would otherwise be wide-ranging searches.

Third, when feasible, such a system of unmonitored recording, accompanied by constrained searches of the footage, might help prevent the kinds of abuses reported by some observers of the United Kingdom’s camera system, where operators have reportedly used cameras for voyeurism or have

533. Solove, *supra* note 343, at 1418 (emphasis added).

534. *New York v. Burger*, 482 U.S. 691, 703 (1987).

535. Senior & Bolle, *supra* note 230, at 90.

536. Jeffrey Rosen reports that current computer scientists are “working on behavioral-recognition technology . . . that can look for unusual movements in crowds” or “stationary loiterers or unaccompanied bags.” ROSEN, *supra* note 29, at 45. Rosen points out that such “behavioral-recognition” technology can be used not only to spot safety threats, but also to lay the groundwork for government harassment of political enemies or citizens’ blackmail of each other. But a system of strict controls on what behavior monitors can observe (and on who can do the observing) could make such nightmarish outcomes less likely by tightly restricting the types of images that an official can access—and by making it very difficult to focus on specific individuals.

focused inordinately on minorities.⁵³⁷ Tightly-circumscribed searches of unmonitored recording after the fact would not present bored camera operators with the opportunity and excuse to spy on innocent behavior or to rely on prejudice to direct their cameras while waiting for evidence of a crime to appear.

Such a two-step system, which allows for a suspicionless search that reveals no new information followed by a more focused and more revealing suspicion-based search, has already been proposed in the context of drug tests.⁵³⁸ As Justice Marshall pointed out in his dissent in *Skinner*, the urinalysis drug testing conducted by the government really involved multiple searches, not just one.⁵³⁹ The first of these searches, the taking of the urine sample itself, did intrude upon a very private activity. The excretory function has traditionally been shielded by great privacy, but urinalysis hardly makes any intrusion into subjects' *informational* privacy because the taking of the sample by itself does not reveal anything about the person providing it. It was only the subsequent chemical testing of the samples that revealed whether drugs were present (and potentially other medical information as well). According to Justice Marshall, even if a warrant was impractical when the samples were taken,

no exigency prevents railroad officials from securing a warrant before chemically testing the samples they obtain. Blood and urine do not spoil if properly collected and preserved, and there is no reason to doubt the ability of railroad officials to grasp the relatively simple procedure of obtaining a warrant authorizing, where appropriate, chemical analysis of the extracted fluids.⁵⁴⁰

537. Jeffrey Rosen recounts the first observation of video voyeurism in his observation of the United Kingdom's camera system and notes that "when you put a group of bored, unsupervised men in front of live video screens and allow them to zoom in on whatever happens to catch their eyes, they tend to spend a fair amount of time leering at women." Rosen, *supra* note 11, at 92. He also recounts Clive Norris's finding that "operators, in addition to focusing on attractive young women, tend to focus on young men, especially those with dark skin." *Id.* Keith A. Rhodes, the chief technologist for the General Accounting Office, has likewise noted that boredom undermines effective use of video surveillance: "Because watching camera screens is both boring and mesmerizing, the attention of most individuals has degenerated to well below acceptable levels after only 20 minutes of viewing." *National Preparedness: Technologies to Secure Federal Buildings: Testimony Before the Subcomm. on Tech. & Procurement Policy of the House Comm. on Gov't Reform*, 107th Cong. (2002) (statement of Keith A. Rhodes, Chief Technologist, Gen. Accounting Office), available at <http://www.gao.gov/new.items/d02687t.pdf>.

538. See *Skinner v. Ry. Labor Executives' Ass'n*, 489 U.S. 602 (1989) (upholding Federal Railroad Administration regulations requiring blood and urine tests of railroad employees involved in major train accidents).

539. *Id.* at 642 (Marshall, J., dissenting).

540. *Id.*; see also *Anonymous Fireman v. City of Willoughby*, 779 F. Supp. 402, 415 (N.D. Ohio 1991) (noting that an HIV test requiring "separate chemical analysis" is a "new search" apart

Following this model, one might suggest that where video surveillance is indispensable, the least privacy-invasive form of it would often involve warrantless automatic and unobserved recording of certain public activities, followed by human scrutiny only when the government could show probable cause to believe particular recordings would reveal evidence of a crime.

*b. Privacy-Protections in Existing Automated Technologies.—*Courts interested in how this two-step model might be applied to video surveillance and biometric technology might find instructive examples in the steps that some public authorities or businesses have already taken to build privacy protections into biometric or tracking systems. There are four types of steps—used in the implementation of both biometric and tracking technologies—that merit close attention from courts examining how the Fourth Amendment might preserve privacy in the public sphere.

One of these steps is for government to ensure that after data is automatically recorded, it is stored securely and in such a way that it can be accessed only by individuals using it for authorized purposes. Such access protections are a standard part of many legislative privacy protections. The Privacy Act of 1974, for example, provides safeguards to ensure that use and dissemination of personal records occurs only for “a necessary and lawful purpose.”⁵⁴¹ While such protections have not played a significant part in search and seizure cases, William Stuntz has argued that when stringent restrictions on search tactics would substantially harm the government’s war on crime or terror, we should give the government significant freedom to search, but “limit what the government does with the information once it has it.”⁵⁴² Christopher Slobogin has likewise proposed that analysis of “storage and dissemination” should be a central factor in determinations of whether a particular video surveillance system is reasonable.⁵⁴³

In recent federal cases on random drug testing, courts have considered safeguards and evidence regarding dissemination in balancing the need for a search and the privacy interest it threatens. In *Board of Education of Independent School District No. 92 of Pottowatomie County v. Earls*, the Court found that a school’s drug testing policy created only a limited threat to student privacy, in part because “the Policy clearly requires that the [drug] test results be kept in confidential files separate from a student’s other

from extraction of blood for the test, and is “subject to a separate analysis under the Fourth Amendment”).

541. Privacy Act of 1974, Congressional Findings and Statement of Purpose, Act of Dec. 31, 1974, P.L. 93-579, § 2, 88 Stat. 1896. The Privacy Act lists conditions for “disclosure” that an agency must satisfy before disclosing a record “to any person, or to another agency.” 5 U.S.C. § 552a(b) (2000).

542. Stuntz, *supra* note 61, at 2183.

543. See Slobogin, *supra* note 38, at 301–05.

educational records and released to school personnel only on a 'need to know' basis."⁵⁴⁴ In *Chandler v. Miller*, the Court noted (before finding the search unreasonable on other grounds) that, in mandatory drug testing of political candidates, the Georgia Legislature "effectively limited the invasiveness of the testing procedure," in large part by ensuring that "the results of the test are given first to the candidate, who controls further dissemination of the report."⁵⁴⁵ To be sure, the Supreme Court has been too willing to give weight to controls on access even when they are vaguely formulated or poorly enforced. In *Earls* itself, the Court was unperturbed by the fact that a teacher had violated the school's confidentiality policy by leaving students' prescription drug lists where other students could view them.⁵⁴⁶ In *Vernonia School District 47J v. Acton*, the school did not even have a specific policy protecting confidential prescription drug information, but the Court nonetheless emphasized that "it may well be that [if the plaintiff had been selected for the random test], the School District would have permitted him to provide the requested information in a confidential manner" and noted that "[n]othing in the Policy" rules out such confidential treatment.⁵⁴⁷ Of course, access and dissemination controls that simply allow authorities to offer confidential treatment are less effective at protecting individual privacy than rules or technologies that require such privacy protections.

Especially in the context of a search technique as potentially threatening to privacy as video surveillance, courts should demand more from institutions than a vague commitment not to make videotapes widely available. At a minimum, they should require, as a normal condition of reasonableness, that agencies which collect video records to fight crime or terrorism do not view or disseminate them without being prepared to justify, to a magistrate or another qualified authority, why such dissemination and use is necessary. Indeed, courts might conclude that adequate protection of private video records demands not only institutional fences against unauthorized access, but also technological protections to ensure that such video records will be relatively safe, even if they are stolen or carelessly released—like the confidential medical information in *Earls*. Thus courts might ensure that the data is encrypted and perhaps protected with passwords

544. 536 U.S. 822, 833 (2002).

545. 520 U.S. 305, 318 (1997). And the dissemination of the drug test results was one of the reasons that Court found the search scheme unreasonable. See *Ferguson v. City of Charleston*, 532 U.S. 67, 78 (2000) (noting that the use of search results by schools or workplaces for internal decisions about institutional privileges "involves a less serious intrusion on privacy than the unauthorized dissemination of such results to third parties").

546. *Earls*, 536 U.S. at 833.

547. 515 U.S. 646, 660 (1995).

or biometric verification procedures that ensure it will be viewed only by authorized users.⁵⁴⁸

Apart from looking at storage and access controls, courts might also learn from a number of other privacy protection measures built into some existing biometric and tracking technologies. One protection is to automatically destroy recorded data a short period of time after it is obtained. Some “intelligent highway” tracking devices, for example, destroy the location data they acquire from cars very soon after its collection.⁵⁴⁹ Such systems have no need to keep individual records once they have gathered information sufficient to provide officials with an overview of how heavily roads are being used. Effective law enforcement may require more individualized information than does traffic control. Police used the E-ZPass electronic toll system to track a kidnapper,⁵⁵⁰ and might have been unable to do so had the kidnapper’s records been purged too quickly. However, even if certain individualized records are retained for crime control, courts might still ask the state to justify retaining any records it wishes to keep for more than a few days—when authorities should be in a position to know whether crimes took place in a certain area and when records are likely to be most relevant for investigating that crime.

Biometric technologies can likewise be designed to automatically purge data that has no connection to the investigation of a serious crime or terrorist threat. As one manufacturer of facial recognition technology has itself suggested, privacy might be protected with a “no match-no memory rule” which ensures that “no audit trail is kept of faces that do not match a criminal or a person under active police investigation” and that “non-matches are

548. Courts might find one possible model for this method of protection in the legislation considered by the California and New Jersey legislatures for protection of biometric identifiers. In S.B. 169, California considered a provision that would have required that “[b]iometric identifier information collected through the use of facial recognition technology shall be encrypted or otherwise secure from unauthorized access.” S.B. 169, 2001 Leg., 2001–2002 Sess. § 1798.89(f) (Ca.) (amended July 5, 2001), *available at* http://www.ibia.org/sb_169_bill_20010705_amended_asm.pdf.pdf. The New Jersey Legislature is considering a bill to create the “Biometric Identifier Privacy Act,” which would require inter alia that a government entity possessing an individual’s biometric identifier “store, transmit, and protect [it] from disclosure using reasonable care and in a manner that is the same or more protective than” the protection afforded other confidential information. *See* Assemb. B. 2448, 2002 Leg., 2002–2003 Sess. § 4(b) (N.J.); S.B. 1915, 2002 Leg., 2002–2003 Sess. § 4(b) (N.J.).

549. *See, e.g.,* Adam Clymer, *Bay Area Traffic Blips Raise Privacy Concerns: A Network of Transponders Will Track More than 200,000 Vehicles—Anonymously, Insist Officials, Who Say They Only Want Data on Traffic Flow*, CHI. TRIB., Aug. 26, 2002, at 2 (noting that, under the Bay Area’s new TravInfo vehicle tracking and traffic management program, “all data about individual cars will be purged from the computers every 24 hours”).

550. *See* Karen Gaudette, *Sensors Will Help Drivers Track Congestion*, SAN DIEGO UNION TRIB., Aug. 9, 2002, at 2 (noting that E-ZPass records helped police solve the kidnapping and murder of a millionaire in New Jersey).

purged instantly.”⁵⁵¹ Such automatic destruction of records would help preserve in public life the impermanence and concomitant spontaneity that emerging camera networks threaten to eliminate.

A third privacy-protecting measure used by new technologies focuses on distinguishing individuals from identities. An “identity” is simply a name or set of characteristics that serves to distinguish one person or group from another. It can consist of one’s real name or face, but it can also consist of an arbitrary string of letters or numbers—for example, a password or e-mail address. Even when machines such as fingerprint scanners or computers register an identity, they might leave persons with anonymity. As Nanavati points out: “an individual is a singular, unique entity—colloquially a person,” but an “identity” or distinguishing character is not synonymous with the individual and “an individual can have more than one identity.”⁵⁵² In cyberspace, for example, people might distinguish themselves from others only with an e-mail address or username.⁵⁵³ One might adopt multiple identities, and these identities might reveal little about the person behind them. Some devices, however, not only reveal an identity, they reveal that identity which uniquely identifies a *specific* individual, across many different institutional environments, and often reveals a significant amount of information about him or her—or at least provides investigators with a good starting point for acquiring such information. Thus, facial recognition technology is often used to tell authorities who it is that is standing in a certain park or street and to give investigators enough information to connect the image in their camera or their video record with a rather detailed portrait of the person. At a minimum, authorities often want to know the name of the person, what he looks like, and if he is dangerous.

Like purging of data, anonymity-preserving measures might be most feasible outside of the law enforcement context. Thus, some “intelligent highway” tracking devices not only often purge data soon after they record it, they also assign an arbitrary identity to a driver or other information that might quickly tell authorities who is at a particular location instead of registering that person’s license plate number.⁵⁵⁴ But even in law enforcement, it

551. Mark G. Milone, *Biometric Surveillance: Searching for Identity*, 57 BUS. LAW. 497, 509–11 (2001) (citing “responsible use principles” proposed by Visionics, a manufacturer of facial recognition software).

552. NANAVATI ET AL., *supra* note 226, at 10–11.

553. As Lawrence Lessig notes: “In real space you reveal your sex, your age, how you look, what language you speak, whether you can see, whether you can hear, how intelligent you are. In cyberspace you reveal only an address, and one that has no necessary relationship to anything else about you.” LESSIG, *supra* note 101, at 33.

554. See, e.g., Clymer, *supra* note 549, at 2 (noting that, according to the managers of TravInfo, as soon as transponders read an individual electronic toll tag, they “assign it a generic identity tag not linked to the car owner’s name or to any other personal information”).

might be feasible for surveillance systems to at least shield the individual behind the identity until police have a high degree of confidence that they need more specific information.

As Nanavati and other writers point out, the design of biometric systems lends itself to drawing such a distinction between identities and individuals.⁵⁵⁵ As noted in the previous discussion of biometrics, existing biometric technologies generally do not require maintaining an image of a person's distinctive fingerprint, facial appearance, or iris scan. They extract certain measurements from a fingerprint, face, or iris, and then later compare these recorded measurements to those in fingerprints, faces, or irises of people who need to be specifically identified, or perhaps simply verified as "authorized users."⁵⁵⁶ As Nanavati points out, one cannot reconstruct a person's actual facial appearance, or for that matter their fingerprint or iris image, from these specific measurements⁵⁵⁷—for the same reason that one cannot reconstruct a 400-page novel from an identifying record which samples every 20th letter.⁵⁵⁸ Consequently, even if a facial recognition system indicates that a person attending a Super Bowl game matches a specific template in its database, it need not tell investigators precisely who this person is by name. Whether it does may well depend on the circumstances. When police are searching for someone who they have very good reasons to believe is affiliated with a terrorist group, they may well want to know immediately the specific individual pinpointed by a match.

Some law-enforcement or intelligence-gathering needs may not require immediate identification of individuals captured by camera. It is by no means clear that government use of facial recognition or other biometric technologies should *ever* be permissible to track certain people who are not already linked to crime or terrorism. Given the possibility of "mission creep," even very limited and legitimate uses of such tracking may quickly transform into grave and impossible-to-contain threats to individual privacy. But if courts are willing to risk such uses of biometric technology, they might at least insist that such surveillance systems conceal the person behind the

555. See, e.g., NANAVATI ET AL., *supra* note 226, at 10–11 (discussing the distinction between identity and individual within the context of biometrics); LESSIG, *supra* note 101, at 33–35 (discussing how the same distinction operates in cyberspace).

556. See *supra* section II(B)(3); NANAVATI ET AL., *supra* note 226, at 11–12; Statement of James L. Wayman, *supra* note 243 ("It is not the fingerprint that is encrypted on [a smart card used for biometric verification]. It is numbers coming from the fingerprint that are put in the code of the card.").

557. NANAVATI ET AL., *supra* note 226, at 13.

558. See *supra* section II(B)(3); see also NANAVATI ET AL., *supra* note 226, at 19 ("An analogy would be to select a string of letters from a page by taking the 10th letter, 20th letter, 30th letter, and so on. You would have a string of characters that, in and of themselves, had no meaning and that could not be used to rebuild the original text.").

“template” until very strong justification is provided for removing this anonymity. For example, if police wish to use biometric technology not to find a known criminal, but to learn more about an unknown perpetrator—like the D.C. sniper—they should not necessarily be allowed to immediately determine the identity of *every* face they record near a particular crime scene or other area of interest. Before permitting such an invasive use of biometric technology, courts might ask whether police can use anonymous data to build a case for individualized suspicion before uncovering the person behind a specific “match.”⁵⁵⁹

Again, unmonitored recording—supplemented by strong warrant requirements—might allow authorities to limit the damage they do to innocent individuals’ privacy and anonymity. Police might run face or license-plate comparisons from unmonitored video taken near two seemingly-connected crime scenes, and then request a warrant to identify, or more closely examine, any faces or license plates that appear near both sites.

Anonymity protections will be at their strongest where the “face print,” fingerprint, or other biometric identifier is not in the possession of the government at all, but rather in the possession of the individual himself. This is how many biometric systems in airports or border areas actually function. Instead of identifying an unknown face to determine if it is dangerous, they verify, using a biometric code on a “smart card”-type authorization card, that the person is in fact the authorized person he claims to be. Such a system spares people from scrutiny, or government tracking, except in the case when the system reveals that they are claiming a false identity.⁵⁶⁰

A fourth privacy protection measure is related to the one just discussed, and that is to ensure that biometric or location data is not aggregated across different environments except when absolutely necessary. Like controls on storage and access, protection against aggregation of data already plays a role in legislative privacy protection. The Computer Matching and Privacy Protection Act of 1988, for example, amended the Privacy Act to require

559. With such a possibility in mind, privacy-conscious computer scientists at Carnegie Mellon University have proposed what they call “k-same” technology, which police might use to learn certain helpful details from visual records without immediately learning the identities of those in these records. See ELAINE NEWTON ET AL., PRESERVING PRIVACY BY DE-IDENTIFYING FACIAL IMAGES 4 (Carnegie Mellon Univ., Sch. of Computer Sci., Tech. Rep. No. CMU-CS-03-119, 2003) (proposing a mechanism by which “face recognition software is restricted,” but details allowing for comparison between different anonymous images remain, so that “society can have both safety and privacy”), available at <http://privacy.cs.cmu.edu/people/sweeney/CMU-CS-03-119-600dpi.pdf>; see also Senior & Bolle, *supra* note 230, at 90 (“Cryptography will go a long way toward privacy-guarding . . .”).

560. As Jeffrey Rosen notes, such a system, unlike a centrally stored one, “doesn’t threaten privacy because it can’t be used for secondary identifications” but only to assure that “I am indeed the person I said I am.” Jeffrey Rosen, *Life After 9/11: Issues Affecting the Courts and the Nation*, 51 U. KAN. L. REV. 219, 242 (2003).

justification from agencies that wished to “match” personal information in one government database with that in another.⁵⁶¹

Analysts of biometrics, such as John Woodward, have suggested that the design or implementation of biometric technologies can facilitate such protections against aggregation.⁵⁶² Different authorities often use different biometric technologies, for example, fingerprint scans as opposed to facial recognition systems. Even the same type of technology might use different templates in different circumstances. The facial recognition system in Virginia Beach may match me to one type of template—generated from an image of my face—while the facial recognition system in another city matches me to a different template, incorporating different facial measures. Every one of these systems may use different templates at different times, and need not reveal that the person detected at Time 1 is the same as the person detected at Time 2 with a different template. Consequently, even if two administrators in two different agencies have a need to pierce my anonymity in particular circumstances—for example, when I enter a sensitive government area or ask for a government benefit—and a need to retain, for some period of time, a record that a “match” was generated, they need not retain these records in a form which makes it simple to determine that the person matched was the same in both settings.

As John Woodward has argued, such “biometric balkanization”—or “biometric diversity” as he described it in another context—makes biometric technology much safer for privacy than it otherwise might be:

If different technologies are used for different situations, citizens will not face the necessity of reporting to the government’s “biometric central” for enrollment. . . . With biometric balkanization, biometric compartmentalization results because only a small part of the individual’s informational whole can be potentially accessed. For example, if a data thief purloins an individual’s hand geometry pattern, she would only at most be able to unlock information compartments that use a hand geometry-based key.⁵⁶³

And the same “compartmentalization” which protects one’s information against a data thief might also help limit an investigator to that which he needs to know. Courts, of course, are not well-qualified to order specific

561. See 5 U.S.C. § 552a(b) (2000) (codifying the conditions under which federal agencies may disclose “any record” to any person or to any other agency in the absence of a written request or consent from “the individual to whom the record pertains”).

562. See Woodward, *supra* note 261, at 140–47 (arguing that by assuring the security as well as the diversity of biometric systems governments can protect individuals’ privacy).

563. *Id.* at 146–47.

agencies to employ specific biometric technologies. The FBI, the TSA, and local police departments will be best placed to decide which technologies are most useful for them, and they may even decide to use or combine multiple biometric technologies. But while courts cannot make these choices for agencies, they can take “biometric balkanization” into account when deciding whether enough privacy protection is built into a specific surveillance technique to make it reasonable under the Fourth Amendment. In deciding whether police can use hand geometry or face recognition prints, for example, a court might examine just how many “doors” into individuals’ private lives such a method will unlock before determining whether its use by a particular agency is acceptable. Courts might also further biometric balkanization by barring agencies from trying to “cross-match” different kinds of biometric measurements or records without first demonstrating a need to do so.

To be sure, even when characterized by all of the privacy protections I have described above, an unmonitored system of recording, similar to a system of monitored recording, would have to be accompanied by safeguards that prevent it from being easily transformed into an instrument of surveillance that is more deeply intrusive. Technological and administrative safeguards must staunchly protect against access to unmonitored recording, except when there is probable cause. And reliable mechanisms would have to exist for ensuring that an investigator who enters a visual database looking for evidence of a serious crime cannot easily overcome the technological hurdles described above and follow a series of “links” to individuals or places that he has no good reason to be investigating. Assuming such safeguards are in place, however, unmonitored recording often may be preferable to systems in which we are routinely watched by government officials and recorded at their discretion.

Of course, such unmonitored recording is only one means of ensuring that new and powerful surveillance technologies leave public spaces safe for private, anonymous, and spontaneous action. Courts can also insist on “warrant substitutes,” minimizing the impact of video surveillance, and selective warrant requirements for particular enhancements of such surveillance. This does not mean that judges should rigidly impose any or all of these requirements in a given situation. Which limitations are appropriate will depend on the nature of the threat that the government faces and the conditions under which a given surveillance technology can succeed in countering it. Moreover, consistent with the outer boundaries set by courts, local communities should have significant input in shaping the crime- or terror-fighting strategies employed by police in their neighborhoods.

Conclusion

In his *Olmstead* dissent, Brandeis underscored the porousness of the Fourth Amendment protections then recognized by the Supreme Court.⁵⁶⁴ He took note of recent technological advances and of the opportunities they created for “[s]ubtler and more far-reaching means of invading privacy.”⁵⁶⁵ “Can it be,” asked Brandeis of the new forms of surveillance, “that the Constitution affords no protection against such invasions of individual security?”⁵⁶⁶

The Supreme Court has already addressed this question in *Katz v. United States*, holding that the Constitution does afford protection against such electronic invasions of individual security, even where they do not involve physical invasions of a home, office, or other private space.⁵⁶⁷ The Court has also adapted the Fourth Amendment to modern developments in another way, adjusting it to new forms of electronic surveillance and to new kinds of threats to safety. For example, the Court has reshaped its Fourth Amendment jurisprudence in situations when a warrant requirement would severely hamper the government’s efforts to detect and stop hijackers,⁵⁶⁸ keep drunk drivers off the highways,⁵⁶⁹ or address drug epidemics.⁵⁷⁰ In such circumstances, it has found alternative constitutional protections like warrants, that guard against arbitrary and unnecessary invasions of privacy, but give the government enough room to address novel and hard-to-detect threats.⁵⁷¹

In the first few years of the twenty-first century, new developments are again challenging both the response to electronic surveillance that the Court made in *Katz* and the response to unusual security threats that the Court made in its “special needs” and administrative search cases. New forms of video surveillance make it possible to subject the whole of public space—every street, park, and highway—to close and on-going scrutiny. New forms of mass terrorism, unpredictable in their method and target, threaten to

564. *Olmstead v. United States*, 277 U.S. 438, 472–74 (1928) (Brandeis, J., dissenting).

565. *Id.* at 473.

566. *Id.* at 474.

567. 389 U.S. 347, 358–59 (1967).

568. *See, e.g., City of Indianapolis v. Edmond*, 531 U.S. 32, 47–48 (2000) (indicating that the Court’s holding that a highway checkpoint violated the Fourth Amendment “does not affect the validity of . . . searches at places like airports . . . , where the need for such measures to ensure public safety can be particularly acute”).

569. *See, e.g., Mich. Dept. of State Police v. Sitz*, 496 U.S. 444, 455 (1990) (upholding a highway sobriety checkpoint as consistent with the Fourth Amendment).

570. *See, e.g., New Jersey v. T.L.O.*, 469 U.S. 325, 347–48 (1985) (permitting warrantless searches for drugs in schools).

571. *See supra* note 482 and accompanying text.

transform all of public life into a tightly monitored high-security zone and make warrantless searching in public space seem more necessary. Both these changes require that the courts think carefully about how the Fourth Amendment's privacy protection can plausibly be extended to the realm of public space, where such constitutional protections are unfamiliar but where people suddenly have a deep need for them. Such changes also make it difficult to continue to maintain, as some commentators do, that people have no reasonable expectation of privacy in public places. Just as Justice Brandeis once chastised the Court majority in *Olmstead* for ignoring wiretapping while providing constitutional protection against other lesser threats,⁵⁷² the invasiveness and inescapability of emerging public camera systems make it hard to understand how courts can invoke the Fourth Amendment to block government officials from rummaging through purses, containers, or suitcases, but ignore the more substantial threat to privacy presented by ubiquitous video surveillance.

Some commentators see in this challenge a new variant of an old Fourth Amendment problem: just as *Olmstead's* formalism once confined the Fourth Amendment's focus to physical searches and prevented it from taking account of electronic eavesdropping, a new variant of this formalism now bars it from taking account of powerful searches in public spaces. Instead of seeing privacy as inhering in a certain environment, they claim, we should follow *Katz* in conceiving of it as attached to "people, not places."⁵⁷³

As I have argued above, however, this is a problematic foundation for Fourth Amendment jurisprudence. People often rely heavily on the place of an activity in determining whether it is private or not. Moreover, deprived of the boundary lines provided by place, courts often resort to factors that weaken privacy protection rather than bolstering it. They examine, for example, whether activity is sufficiently "intimate" to merit Fourth Amendment protection, a decision which in turn requires controversial, and often poorly informed, judgments about what law-abiding activities people should and should not have a right to shield from others' view.

As I have argued in this Article, there is a more promising response to emerging systems of video surveillance, one which—instead of rejecting the link that *Olmstead* assumed between privacy and the location or environment of an activity—revives and reconceptualizes this link. Just as courts have protected (and continued to protect) the home as an environment for private action, courts should also protect those features of public space that allow for

572. 277 U.S. 438, 474–77 (Brandeis, J., dissenting) (describing how the Court had previously held that opening letters without a warrant violated the Fourth Amendment).

573. *Katz v. United States*, 389 U.S. 347, 351 (1967).

a different sort of private and anonymous action in that realm. For while the home is perhaps the most crucial enclave for private action, it is not the only indispensable one. People also need privacy and anonymity in many aspects of public life—for example, when they explore controversial films, books, or ideas, have conversations in public places, or seek aid or counsel of a sort they can only find by venturing into the public sphere. Although walls and windows do not shield these public activities from everyone's view, other features of physical and social architecture, *distinctive* to public space, do shield them. Crowds and the diversity and separateness of the social circles that people move in allow people to find anonymity; the existence of isolated and unmonitored islands of public space allow them to find seclusion; and the evanescent nature of the appearance that they present to the world at any one moment gives them freedom to reinvent themselves. These privacy-protecting features of public space cannot easily survive in a world of ubiquitous cameras, and the task of preserving them requires courts to do in a sense the opposite of what *Katz* recommends: They must abandon the task of identifying difficult-to-identify expectations of privacy, abandon the complex, multifactor judgments about when these expectations are justified, and instead return to the task of preserving the environment that makes privacy possible.

* * *

Feds to study illegal use of spy gear



By **Craig Timberg** August 11, 2014

The Federal Communications Commission has established a task force to study reported misuse of surveillance technology that can intercept cellular signals to locate people, monitor their calls and send malicious software to their phones.

The powerful technology -- called an IMSI catcher, though also referred to by the trade name “Stingray” — is produced by several major surveillance companies and widely used by police and intelligence services around the world.

The FCC, in response to questions from U.S. Rep. Alan M. Grayson (D-Fla.), plans to study the extent to which criminal gangs and foreign intelligence services are using the devices against Americans. FCC Chairman Tom Wheeler, in a letter dated this month, said the commission had authority over the surveillance technology and had established a “task force to combat the illicit and unauthorized use of IMSI catchers.”

The task forces's mission, Wheeler wrote, "is to develop concrete solutions to protect the cellular network systemically from similar unlawful intrusions and interceptions.”

The action followed numerous news reports, in Newsweek, the Harvard Journal of Law and Technology and The Washington Post, about the vulnerability of cellular networks to interception. Grayson cited those reports in noting that IMSI catchers could be bought for as little as \$1,800, or built by anybody with a moderate degree of technical expertise.

The devices work by mimicking cell towers to trick nearby phones to route their data through the IMSI catcher. Though some cellular traffic is encrypted, IMSI catchers often are marketed with systems for cracking common forms of encryption.

The Switch newsletter

The day's top stories on the world of tech.

[Sign up](#)

“Americans have a reasonable expectation of privacy in their communications, and in information about where they go and with whom they communicate,” Grayson wrote to Wheeler in July. “It is extremely troubling to learn that cellular communications are so poorly secured, and that it is so easy to intercept calls and track people’s phones.”

The widespread use of IMSI catchers by law enforcement also has prompted significant legal debates, with civil liberties groups arguing that police have too much latitude in collecting data that flows through cellular networks.

Stephanie K. Pell, a cyber-ethics fellow at the Army Cyber Institute at the U.S. Military Academy, said the FCC should investigate not only the illegal uses of IMSI catchers but the network vulnerabilities that allow them to work.

“I think it would be prudent to assume that the Chinese government and criminal gangs don’t care if IMSI catchers are illegal,” said Pell, who has written extensively about the technology. “Ultimately if we are going to get to the root of the problem, we will have to deal with this from a network vulnerability perspective.”

Pell said her views were personal and did not represent those of the Army Cyber Institute.

Craig Timberg is a national technology reporter for The Post. 🐦 Follow @craigtimberg

PAID PROMOTED STORIES

Recommended by  Outbrain



This Brand New Fit Minimizes Your Frames From Sliding

Warby Parker



Chancellor does the impossible against Gronkowski - ESPN Video

ESPN



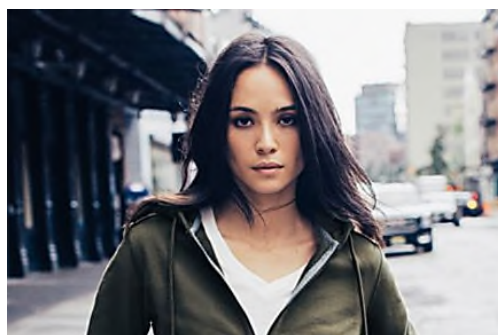
How 2 Boston Grads Are Disrupting the Auto Insurance Industry

EverQuote



Donald Trump's Advice For Paying Off Mortgage (It's Genius!)

Bills.com



An Apple engineer designed a sweatshirt that's disrupting American Manufacturing

American Giant



Do This Every Time You Turn On Your Computer...

www.weblifeadvice.com

What Happens When the Surveillance State Becomes an Affordable Gadget?

Maybe it doesn't faze you that your local police have a \$400,000 device that listens in on cell phones. How will you feel when your neighbor has a \$1,500 version?

Robert Kolker

[Subscribe Reprints](#)

BloombergBusinessweek

March 10, 2016 — 5:00 AM CST

Updated on March 10, 2016 — 10:05 AM CST

When Daniel Rigmaiden was a little boy, his grandfather, a veteran of World War II and Korea, used to drive him along the roads of Monterey, California, playing him tapes of Ronald Reagan speeches. Something about the ideals of small government and personal freedom may have affected him more deeply than he realized. By the time Rigmaiden became a disaffected, punk-rock-loving teenager, everything about living in America disappointed him, from the two-party system to taxes. “At that age, everybody’s looking for something to rebel against,” he tells me over Mexican food in Phoenix—where, until recently, he was required to live under the conditions of his parole. “I thought, ‘I either have to fight the rigged system, or I have to opt out completely.’ ”

Rigmaiden is 35 and slender, quiet with a sardonic smile and thick shock of jet-black hair. Speaking softly and rapidly, he tells the story of how he evolved from a bottom-feeding Internet outlaw to one of the nation’s most prescient technological privacy activists. Rigmaiden left home in 1999 after graduating high school and spent almost a decade knocking around college towns in California, living under a series of assumed names. “I didn’t want to be constrained by all the rules of society,” he says. “It just didn’t seem real to me.” He’d spend weeks living in the woods, scrounging for food and water, testing his limits; then he’d find a place to crash for a while and make a little money on the Internet—first selling fake IDs, then moving on to more serious crimes. In 2006 he wrote software to mine information from databases on the Internet—names, birthdates, Social Security numbers, and the employer identification numbers of businesses. Then he filed fake tax returns, hundreds of them, collecting a modest refund with each.

He bought gold coins with cash, built a nest egg of about \$500,000, and planned to move to South America when the time was right. Then, in 2008, an FBI, IRS, and U.S. Postal Service task force grabbed Rigmaiden at his apartment in San Jose and indicted him on enough wire fraud and

identity theft charges to put him away for the rest of his life. Only after he was caught did the authorities learn his real name.

The mystery, at least to Rigmaiden, was how they found him at all. He'd been living completely off the grid. The only thing connecting him to the world outside his apartment, he knew, was the wireless AirCard of his laptop. To find him, he reasoned, the people who caught him would have had to pluck the signal from his particular AirCard out of a wilderness of other signals and pinpoint his location. To do that, they'd need a device that, as far as he knew, didn't exist.

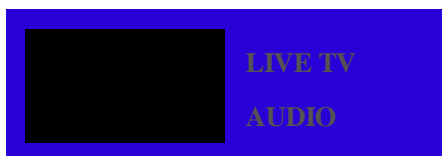


Rigmaiden, fraudster turned privacy advocate.

Photographer: Nick Cote/NYTimes/Redux

Rigmaiden made it his mission to find out what that device was. He was jailed but never tried; he slowed down the process by filing endless motions contesting his arrest, insisting he'd been essentially wiretapped without a warrant. In the prison library, he became a student of telecommunications. Among the most important things he learned was that whenever a cell phone communicates with a cell tower, it transmits an International Mobile Subscriber Identity, or IMSI. His AirCard, like a cell phone, had an IMSI. He reasoned that the government had to have a gadget that masqueraded as a cell tower, tricking his AirCard into handing over its IMSI, which was then matched up to the IMSI connected to all his online phony tax filings. It was all inference, at first, but if it was true, that would be enough for him to make the case that what was done to his AirCard was an illegal search.

It took two years before Rigmaiden found the first real glimmer of proof. He was plowing through a stash of records the Electronic Frontier Foundation had unearthed in the files of the



System Network—the bureau's technological communications unit. He noticed a mention of a Wireless Intercept and Tracking Team, a unit

set up specifically for targeting cell phones. He connected what he found there to an agenda he'd found from a city council meeting in Florida in which a local police department was seeking permission to buy surveillance equipment. The attachment gave the equipment a name: StingRay, made by Harris Corp.

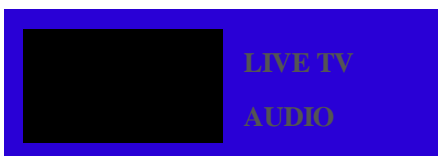
The StingRay is a suitcase-size device that tricks phones into giving up their serial numbers (and, often, their phone calls and texts) by pretending to be a cell phone tower. The technical name for such a device is IMSI catcher or cell-site simulator. It retails for about \$400,000. Harris and competitors like Digital Receiver Technology, a subsidiary of Boeing, sell IMSI catchers to the military and intelligence communities, and, since 2007, to police departments in Los Angeles, New York, Chicago, and more than 50 other cities in 21 states. The signals that phones send the devices can be used not just to locate any phone police are looking for (in some cases with an accuracy of just 2 meters) but to see who else is around as well. IMSI catchers can scan Times Square, for instance, or an apartment building, or a political demonstration.

Rigmaiden built a file hundreds of pages thick about the StingRay and all its cousins and competitors—Triggerfish, KingFish, AmberJack, Harpoon. Once he was able to expose their secret use—the FBI required the police departments that used them to sign nondisclosure agreements—the privacy and civil-liberties world took notice. In his own case, Rigmaiden filed hundreds of motions over almost six years until he finally was offered a plea deal—conspiracy, mail fraud, and two counts of wire fraud—in exchange for time served. He got out in April 2014, and his probation ended in January. Now Rigmaiden is a free man, a Rip Van Winkle awakening in a world where cell phone surveillance and security is a battleground for everyone.

In the ongoing scrum over cell phone privacy, there are at least two major fields of play: phone-data encryption, in which, right now, Apple is doing its best not to share its methods with the government; and network security, in which the police and the military have been exploiting barn-door-size vulnerabilities for years. And it's not just the government that could be storming through. The same devices the police used to find one low-rent tax fraudster are now, several years later, cheaper and easier to make than ever.

"Anybody can make a StingRay with parts from the Internet," Rigmaiden tells me, citing a long litany of experiments over the years in which researchers have done just that. "The service provider is never going to know. There's never any disruption. It's basically completely stealth." In the coming age of democratized surveillance, the person hacking into your cell phone might

I. It could be your next-door neighbor.



It might not be the police or the FBI. It could be your neighbor

In February, on a snowy morning in Annapolis, Md., a panel of three judges is hearing arguments in the first StingRay case to make it to an appeals court. It's the case of Kerron Andrews, a 25-year-old man arrested two years ago in Baltimore for attempted murder. His court-appointed lawyer did what a lot of court-appointed lawyers in Baltimore have been doing in recent years: Inspired by the Rigmaiden case, she contested his arrest on Fourth Amendment grounds, arguing that the technology used to apprehend the suspect was not specified in the court order allowing the police to search for him at a particular house. At first, prosecutors said they could not confirm that any technology was used at all—those nondisclosure agreements have kept more than one police department quiet—but eventually they conceded that the police found Andrews with a Hailstorm, a next-generation version of the StingRay, also built by Harris. When a judge tossed out most of the evidence in the case, the state appealed, making *Maryland v. Andrews* the first IMSI catcher case to potentially make sweeping case law at the appellate level.

During arguments, at least two of the three appellate judges on the panel appear skeptical of the state's case. Judge Daniel Friedman seems exasperated that the police and prosecutors didn't seem to understand the Hailstorm well enough to know if it was intruding on the privacy of suspects. Judge Andrea Leahy suggests that this case fits tidily into the Supreme Court's 2012 decision *USA v. Jones*, which ruled that the police could not install a GPS device on someone's car without a warrant. "Wiretaps require warrants," she says.

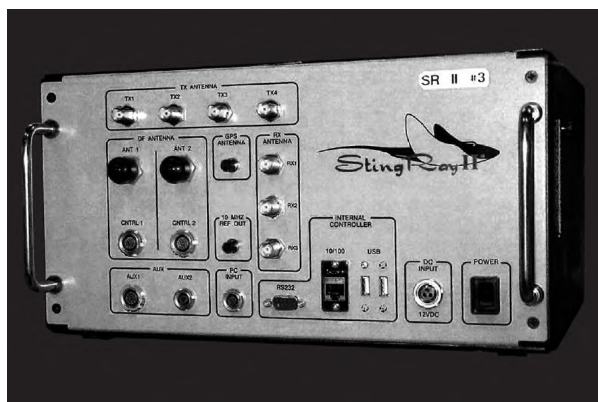
Then Daniel Kobrin, the appellate lawyer representing Andrews, argues, in a way that would make Tim Cook proud, that Hailstorm violates everyone's reasonable expectation of privacy. Unlike, say, the garbage you'd leave outside your house, Kobrin says, there's nothing about a phone that is thought of as fair game for the police. "When I have my phone and I'm walking down the street, I'm not telling my phone to let Verizon or Sprint or T-Mobile know where I am," the lawyer says. "Phones are not tracking devices. Nobody buys them for that reason. Nobody uses them for that reason." A few weeks later, the panel would affirm the lower court's decision to suppress evidence seized as a result of the use of the Hailstorm. Soon, Maryland may have to

state and require explicit language in its warrants about the use of any clients.

LIVE TV
AUDIO

Watching the proceedings from the gallery is Christopher Soghoian, the principal technologist for the American Civil Liberties Union. He, even more than Rigmaiden, may be the person most responsible for exposing the vulnerability of the telecommunications system to surveillance and goading the states, one by one, to regulate its use. A bearded, long-haired Ph.D. from Indiana University, Soghoian has been raising the alarm about the StingRay for five years—ever since he got a message sent by Rigmaiden from prison saying he could prove the police hacked his phone. “I remembered seeing it in *The Wire*,” Soghoian says, “but I thought that was fictional.” (Phone-tracing gadgets are a television staple, also popping up in *Homeland*.) Soghoian’s colleagues educated dozens of public defenders in Maryland about the police’s favorite toy; in one case last summer, a detective testified that the Baltimore police have used a Hailstorm some 4,300 times. “That’s why there are so many StingRay cases in Baltimore,” Soghoian tells me. “Because the defense lawyers were all told about it.”

Harris is a publicly traded Florida-based defense contractor with a \$9.7 billion market cap and 22,000 employees. In the 1970s, Harris built the first secured hotline between the White House and the Kremlin; later it branched out into GPS, air traffic management, and military radios. Harris’s first visible foray into cell-site simulation was in 1995, when the FBI used the Harris-made Triggerfish to track down the notorious hacker Kevin Mitnick, who, in his time, seized proprietary software from some of the nation’s largest telecom companies.

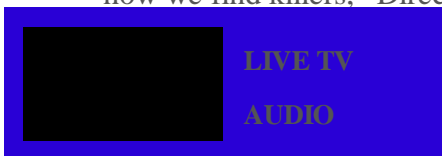


The StingRay II

Source: U.S. Patent and Trademark Office/AP Photo

The StingRay arrived a few years later—an update of Triggerfish designed for the new digital cellular networks. The first clients were soldiers and spies. The FBI loves IMSI catchers—“It’s how we find killers,” Director James Comey has said—even if last fall, under pressure after

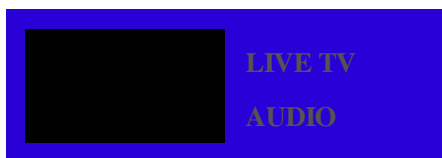
rs became public, the Justice Department announced that the FBI warrants before using them.



Most local police departments, though, still aren't bound by that directive. Neither are foreign governments, which are widely suspected to be using IMSI catchers here (as we are no doubt doing elsewhere). And so, amid the publicity over the StingRay, a marketplace has opened up for countermeasures. On the low end, there's SnoopSnitch, an open source app for Android that scans mobile data for fake cell sites. On the high end, there's the CryptoPhone, a heavily tricked-out cell phone sold by ESD America, a boutique technology company out of Las Vegas. The \$3,500 CryptoPhone scans all cell-site signals it's communicating with, flagging anything suspicious. Even though the CryptoPhone cannot definitively verify that the suspect cell is an IMSI catcher, "we sell out of every CryptoPhone we have each week," says ESD's 40-year-old chief executive officer, Les Goldsmith, who has marketed the phone for 11 years. "There are literally hundreds of thousands of CryptoPhones globally." ESD's dream clients are nations. Last year the company debuted a \$7 million software suite called OverWatch, developed with the German firm GSMK. OverWatch, ESD says, can help authorities locate illegal IMSI catchers using triangulation from sensors placed around a city. "Right now, it's going into 25 different countries," Goldsmith says.

On a parallel track to the defense market, hobbyists and hackers have gone to work on the cell networks and found they can do a lot of what Harris can. In the early days of cell phones, when the signals were analog, like radio, DIY phone-hacking was a cinch. Anyone could go to a RadioShack and buy a receiver to listen in on calls. Congress grew concerned about that and in the 1990s held hearings with the cellular industry. It was an opportunity to shore up the networks. Instead, Congress chose to make it harder to buy the interception equipment. The idea was that when digital mobile technology took hold, intercepting digital signals would be just too expensive for anyone to bother trying. That turned out to be more than a little shortsighted.

For as long as you've been using a phone on a 2G (also called GSM) network or any of its digital predecessors, your calls, texts, and locations have been vulnerable to an IMSI catcher. In 2008 researcher Tobias Engel became the first to demonstrate a crude homemade IMSI catcher, listening to calls and reading texts on a pre-2G digital cell network. Two years later, at a DEF CON hacking conference in Las Vegas, researcher Chris Paget monitored calls made on 2G with a gadget built for just \$1,500. What made it so cheap was "software-defined radio," in which all the complicated telecommunications tasks aren't pulled off by the hardware but by the software. If you couldn't write the software yourself, someone on the Internet had probably already done it for you.



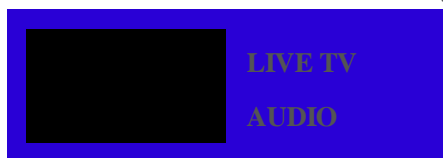
more sophisticated 3G and 4G (also known as LTE) networks. In theory, only the location of these phones, not listen to calls or read texts. But

none of that matters if the IMSI catcher in question can just knock a phone call back down to 2G. Enter Harris's Hailstorm, the successor to StingRay. "It took us a while to stumble onto some documents from the DEA to see that the Hailstorm was a native LTE IMSI catcher," the ACLU's Soghoian says. "It was like, 'Wait a second—I thought it's not supposed to work on LTE. What's going on?'"

They found a hint to the answer last fall, when a research team out of Berlin and Helsinki announced it had built an IMSI catcher that could make an LTE phone leak its location to within a 10- to 20-meter radius—and in some cases, even its GPS coordinates. "Basically we downgraded to 2G or 3G," says Ravishankar Borgaonkar, a 30-year-old Ph.D. who has since been hired at Oxford. "We wanted to see if the promises given by the 4G systems were correct or not." They weren't. The price tag for this IMSI catcher: \$1,400. As long as phones retain the option of 2G, calls made on them can be downgraded. And the phone carriers can't get rid of 2G—not if they want every phone to work everywhere. The more complex the system becomes, the more vulnerable it is. "Phones, as little computers, are becoming more and more secure," says Karsten Nohl, chief scientist at Security Research Labs in Berlin. "But the phone networks? They're rather becoming less secure. Not because of any one action but because there's more and more possibility for one of these technologies to be the weakest link."

The device Borgaonkar's team built is called a "passive receptor," a sort of budget StingRay. Instead of actively targeting a single cell phone to locate, downgrade to 2G, and monitor, a passive receptor sits back and collects the IMSI of every cell signal that happens by. That's ideal for some police departments, which, the *Wall Street Journal* reported last summer, have been buying passive devices in large numbers from KEYW, a Hanover, Md., cybersecurity company, for about \$5,000 a pop. One Florida law enforcement document described the devices as "more portable, more reliable and 'covert' in functionality." If all you want to do is see who's hanging out at a protest—or inside a house or church or drug den—these passive receptors could be just the thing.

A programmer I spoke with who has worked for Harris is of two minds about what the hobbyists are up to. "There's a giant difference between do-it-yourself IMSI catchers and something like the Harris StingRay," he says proudly. That said, he's taken with how fast the amateurs are catching up. "I'd say the most impressive leap is the advancement of LTE support on software-defined radio," he says. "That came out of nowhere. From nothing to 2G took, like, 10 years, and from 2G to LTE took five years. We're not there yet. But they're coming. They're definitely



No one wants to fix the problem—they exploit the vulnerability, too

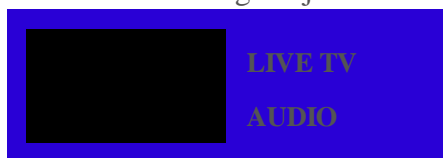
You don't have to look far to see what a world of cheap and plentiful IMSI catchers looks like. Two years ago, China shut down two dozen factories that were manufacturing illegal IMSI catchers. The devices were being used to send text-message spam to lure people into phishing sites; instead of paying a cell phone company 5¢ per text message, companies would put up a fake cell tower and send texts for free to everyone in the area.

Then there's India. Once the government started buying cell-site simulators, the calls of opposition-party politicians and their spouses were monitored. "We can track anyone we choose," an intelligence official told one Indian newspaper. The next targets were corporate; most of the late-night calls, apparently, were used to set up sexual liaisons. By 2010 senior government officials publicly acknowledged that the whole cell network in India was compromised. "India is a really sort of terrifying glimpse of what America will be like when this technology becomes widespread," Soghoian says. "The American phone system is no more secure than the Indian phone system."

In America, the applications are obvious. Locating a Kardashian (in those rare moments when she doesn't want the media to locate her) is something any self-respecting TMZ intern would love to be able to do. "What's the next super Murdoch scandal when the paparazzi are using a StingRay instead of hacking into voicemail?" Soghoian says. "What does it matter that you can build one for \$500 if you can buy one for \$1,500? Because at the end of the day, the next generation of paparazzi are not going to be hackers. They're going to be reporters with expense accounts."

Over coffee after court in Annapolis, Soghoian and I peruse the Alibaba.com marketplace on his smartphone. He types in "IMSI catcher," and a list materializes. The prices are all over the place, as low as \$1,800. "This one's from Nigeria. ... This one's \$20,000. ... This one's from Bangladesh." I note that the ones on sale here seem to work only on 2G, unlike the Hailstorm. "You can get a jammer for like 20 bucks," Soghoian says. With that, you roll any call back to 2G.

With a cheap old IMSI catcher, and you've got a crude facsimile of a



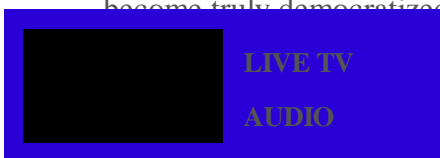
Every country knows it's vulnerable, but no one wants to fix the problem—because they exploit that vulnerability, too. Two years ago, Representative Alan Grayson (D-Fla.) wrote a concerned letter to the Federal Communications Commission about cellular surveillance vulnerabilities. Tom Wheeler, the former industry lobbyist who now runs the regulatory agency, convened a task force that so far has produced nothing. “The commission’s internal team continues to examine the facts surrounding IMSI catchers, working with our federal partners, and will consider necessary steps based on its findings,” says FCC spokesman Neil Grace.

Soghoian isn't optimistic. “The FCC is sort of caught between a rock and a hard place,” he says. “They don't want to do anything to stop the devices that law enforcement is using from working. But if the law enforcement devices work, the criminals' devices work, too.” Unlike the battle between the FBI and Apple, the network-vulnerability struggle doesn't pit public sector against private; it's the public sector against itself.

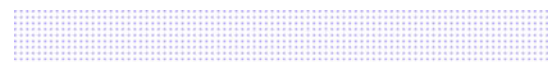
“There are lots of people who want to spy on their neighbors or their spouses or their girlfriends”

From his apartment in central Phoenix, Rigmaiden consulted with the Washington state branch of the ACLU when it helped draft the state law requiring a warrant for the use of IMSI catchers. He's suing the FBI for more StingRay documents, and recently the court shook loose a few more. And now that his parole is over and he can travel, he'd like to lecture across the country about fighting surveillance. “Everything that I thought was wrong back then is even worse today,” he says, chuckling softly. “The only thing that's changed is now I'm going to do the other route—which is participate and do what I can to try to change it.”

As improbable a privacy standard bearer as Rigmaiden may be, his ability to draw inferences and connect dots proved useful once; maybe it will again. He has dug up the specs of some KEYW passive devices, and he sees no reason the big companies like Harris aren't already miles beyond that now. “Every beat cop, every police car on every police force is going to have one of these passive interceptors in the car or on their utility belt,” Rigmaiden says. For surveillance to become truly democratized, he reasons, “it has to be as easy as installing an app on your phone. I would have to decide, I'm going to make this easy for people to do.



He's hardly alone in this view. "The next step for the technology is to go into the hands of the public, once it gets cheap enough," says Jennifer Lynch, a staff attorney at the Electronic Frontier Foundation. "Companies are always going to try to find new markets for their technologies. And there are lots of people who want to spy on their neighbors or their spouses or their girlfriends."



Close all those tabs. Open this email.

Get Bloomberg's daily newsletter.

Enter your email	Sign Up
------------------	---------



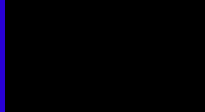
Meanwhile, apart from IMSI catchers, a whole other vulnerability has been exposed: Companies such as Verint Systems and Defentek have produced devices that exploit a huge security hole in SS7 (short for Signaling System 7), the network that interconnects every cellular provider around the world. Using SS7, researchers on laptops have been able to pinpoint the location of a particular cell phone anywhere in the world—and even intercept calls. The attacker does leave an IP

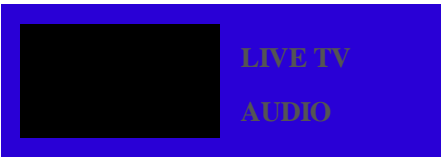
address as a trace. "But if that IP address leads somewhere like Russia or China," says Tobias Engel, who cracked SS7 in a 2014 demonstration in Hamburg, "you really don't know much more." The industry lobbying group CTIA—The Wireless Association maintains that SS7 is more secure in America than in Europe. "Outside the U.S., the networks are more fragmented, not as homogeneous," says John Marinho, who runs the group's cybersecurity working group.

Goldsmith of ESD—which has developed another multimillion-dollar software package, called Oversight, aimed at warding off SS7 attacks—disagrees. "That's comical," he says. "I can tell you we performed tests on U.S. carriers, and they're just as vulnerable as anyone else."

What fascinates Rigmaiden the most—and what sometimes makes him want to go live in the woods again—is how no matter what happens with Apple's battle, the cell phone network problem may be with us for as long as there are networks. "This isn't something that can really be fixed," he says. "It's just built into the way communications work. You can always zero into one signal among many signals, if you have enough data. You don't need to hack anything—just analyze the signals in the air."

(Corrects Soghoian's alma mater in the 14th paragraph.)

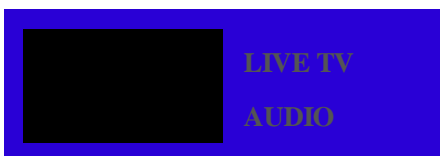
 LIVE TV AUDIO	Subscribe now to BloombergBusinessweek
--	---



[Terms of Service](#) [Trademarks](#) [Privacy Policy](#)

©2016 Bloomberg L.P. All Rights Reserved

[Careers](#) [Made in NYC](#) [Advertise](#) [Ad Choices](#) [Website Feedback](#) [Help](#)



Protect Our Rights

We Need You to Stand With Us Now

Donate

ACLU

ELECTION '16 

GET UPDATES

DONATE



MULTIMEDIA

Stingray Tracking Devices: Who's Got Them?

The map below tracks what we know, based on press reports and publicly available documents, about the use of stingray tracking devices by state and local police departments. Following the map is a list of the federal agencies known to have the technology. The ACLU has identified 68 agencies in 23 states and the District of Columbia that own stingrays, but because many agencies continue to shroud their purchase and use of stingrays in secrecy, this map dramatically underrepresents the actual use of stingrays by law enforcement agencies nationwide.

Stingrays, also known as "cell site simulators" or "IMSI catchers," are invasive cell phone surveillance devices that mimic cell phone towers and send out signals to trick cell phones in the area into transmitting their locations and identifying information. When used to track a suspect's cell phone, they also gather information about the phones of countless bystanders who happen to be nearby.

MORE ON STINGRAY TRACKING DEVICES 

Related Issues: Stingray Tracking Devices, Surveillance Technologies, Privacy & Technology, Privacy and Surveillance, National Security



Click any highlighted state to learn more

ACLU

SHOW MAP DATA +

ALASKA

Local police have cell site simulators

Local Police

- Anchorage Police Department

ALABAMA

Police use of cell site simulators unknown

ARKANSAS

Police use of cell site simulators unknown

ARIZONA

Local police have cell site simulators

Local Police

- Tucson Police Department
 - Maricopa County Sheriff: "'Stingray' Phone Tracker Fuels Constitutional Clash" (Wall Street Journal)
 - Tempe
 - Gilbert Police Department (Possible)
 - Phoenix Police Department (Center for Human Rights and Privacy)
 - Scottsdale Police Department (Center for Human Rights and Privacy)
-

CALIFORNIA

Local and state police have cell site simulators

Local Police

- San Diego Police Department: "Local police dealt with company that makes controversial cellphone tracking technology" (ABC News 10)
- San Jose Police Department, Oakland Police Department,

San Diego Sheriff's Department, San Francisco Police Department, Los Angeles Sheriff's Department, Los Angeles Police Department, and Sacramento County Sheriff: "9 Calif. law enforcement agencies connected to cellphone spying technology" (ABC News 10)

- Los Angeles Police Department: "LAPD Spy Device Taps Your Cell Phone" (LA Weekly)

- San Bernadino County Sheriff: "Law enforcement officials: Cell phone disclosures would hurt investigations" (Desert Sun)

- Ventura County Sheriff (Center for Human Rights and Privacy)

- Anaheim Police Department (ACLU of Northern California)

State Police

- California Department of Justice (Center for Human Rights and Privacy)

COLORADO

Police use of cell site simulators unknown

CONNECTICUT

Police use of cell site simulators unknown

DISTRICT OF COLUMBIA

Local police have cell site simulators

Local Police

- Washington, DC, Metropolitan Police Department: "Police in Washington, DC Are Using the Secretive 'Stingray' Cell Phone

Tracking Tool" (Vice News)

DELAWARE

State police have cell site simulators

State Police

- Delaware State Police (FOIA Response to Mike Katz-Lacabe)
-

FLORIDA

Local and state police have cell site simulators

Local Police

- Miami-Dade Police Department: "Cell-phone tracking: Miami cops know where you are" (Miami New Times)
- City of Miami Police Department
- Sunrise Police Department

State Police

- Florida Department of Law Enforcement (FDLE loans cell site simulators to local and county police departments throughout the state)
-

GEORGIA

Local police have cell site simulators

Local Police

- Gwinnett County Police
-

HAWAII

Police use of cell site simulators unknown

IDAHO

Police use of cell site simulators unknown

ILLINOIS

Local and state police have cell site simulators

Local Police

- [Chicago Police Department: "Lawsuit seeks details on Chicago Police purchases of cellular tracking gear"](#) (Chicago Sun-Times)
- [After Denials Chicago Police Department Admits Purchase Of Cell-Phone Spying Devices](#) (CBS Chicago)

State Police

- [Illinois State Police](#)
-

INDIANA

State police have cell site simulators

State Police

- [Indiana State Police: "Indiana State Police tracking cellphones — but won't say how or why"](#) (Indianapolis Star)
-

IOWA

Police use of cell site simulators unknown

KANSAS

Police use of cell site simulators unknown

KENTUCKY

Police use of cell site simulators unknown

LOUISIANA

State police have cell site simulators

State Police

- [Louisiana Attorney General: 9News Investigators: Phishing in your phone \(WAFB\)](#)

MAINE

Police use of cell site simulators unknown

MARYLAND

Local and state police have cell site simulators

Local Police

- [Montgomery County](#)
- [Baltimore](#)
- [Baltimore County: "Baltimore Co. Police Used Secretive Phone-Tracking Technology 622 Times" \(Baltimore Sun\)](#)
- [Anne Arundel County I & II](#)
- [Prince George's County: "Asset Seizures Fuel Police Spending" \(Washington Post\)](#)
- [Annapolis: Battlefield Technology Gets Spotlight in Maryland Courts \(Capital News Service\)](#)
- [Hartford County \(Capital News Service\)](#)

- Howard County: Battlefield Technology Gets Spotlight in Maryland Courts (Capital News Service)

State Police

- Maryland State Police

MASSACHUSETTS

Local police have cell site simulators

Local Police

- Boston Police Department (via Center for Human Rights and Privacy)

MICHIGAN

Local and state police have cell site simulators

Local Police

- Oakland County Sheriff: "Secret military device lets Oakland deputies track cellphones" (Detroit News)

State Police

- Michigan State Police

MINNESOTA

Local and state police have cell site simulators

Local Police

- Hennepin County Sheriff: "This time, Stanek lands KingFish phone tracker" (Star Tribune)

State Police

- Minnesota Bureau of Criminal Apprehension: "BCA still

keeps quiet about cell tracking technology----admit have
Stingray" (Open Secrets)

MISSISSIPPI

Police use of cell site simulators unknown

MISSOURI

Local police have cell site simulators

Local Police

- St. Louis Police Department
 - Kansas City Police Department: "Secret cellphone tracking device used by police stings civil libertarians" (Kansas City Star)
-

MONTANA

Police use of cell site simulators unknown

NEBRASKA

Police use of cell site simulators unknown

NEVADA

Police use of cell site simulators unknown

NEW HAMPSHIRE

Police use of cell site simulators unknown

NEW JERSEY

Police use of cell site simulators unknown

NEW MEXICO

Police use of cell site simulators unknown

NEW YORK

Local and state police have cell site simulators

Local Police

- [New York City Police Department \(NYPD\)](#) (New York Civil Liberties Union)
- [Erie County Sheriff: "Erie Co. Sheriff Spent \\$350,000 To Spy On Cell Phones"](#) (WGRZ TV)
- [Rochester Police Department](#) (New York Civil Liberties Union)

State Police

- [New York State Police: "Local Police Agencies Have Devices to Spy on Cell Phones"](#) (WGRZ TV)
-

NORTH CAROLINA

Local and state police have cell site simulators

Local Police

- [Charlotte Police Department I & II](#)
- [Durham Police Department](#)

- Raleigh Police Department: "Raleigh, Durham police using device that tracks cellphone data" (WRAL)
- Wilmington Police Department
- New Hanover Sheriff's Department (Daily Dot)

State Police

- North Carolina State Bureau of Investigation (Daily Dot)
-

NORTH DAKOTA

Police use of cell site simulators unknown

OHIO

Police use of cell site simulators unknown

OKLAHOMA

State police have cell site simulators

State Police

- Oklahoma Bureau of Narcotics and Dangerous Drugs: Okla. Authorities Have or Use Controversial Cellphone Tracker (Oklahoma Watch)
-

OREGON

Police use of cell site simulators unknown

PENNSYLVANIA

State police have cell site simulators

State Police

- [Pennsylvania State Police: "Confirmed: PA State Police Purchased Controversial StingRay Surveillance Technology Last Year"](#) (The Declaration)
-

RHODE ISLAND

Police use of cell site simulators unknown

SOUTH CAROLINA

Police use of cell site simulators unknown

SOUTH DAKOTA

Police use of cell site simulators unknown

TENNESSEE

Local police have cell site simulators

Local Police

- [Memphis Police Department](#)
 - ["MPD May Be Using New Data Collection Program"](#) (LocalMemphis.com)
-

TEXAS

Local and state police have cell site simulators

Local Police

- [Fort Worth Police Department: "Fort Worth Cellphone Tracker Rings Controversy"](#) (NBC 5)

- Houston Police Department

State Police

- Texas Department of Public Safety: "APD: Can We Please Buy Some Top-Secret 'Stingrays'?" (Austin Chronicle)

UTAH

Police use of cell site simulators unknown

VERMONT

Police use of cell site simulators unknown

VIRGINIA

Local police have cell site simulators

Local Police

- Alexandria Police Department (possible)
- Chesterfield Police Department
- Fairfax County Police Department: "DC, Maryland, and Virginia cops spying on cell phone data" (WUSA 9)

WASHINGTON

Local police have cell site simulators

Local Police:

- Tacoma Police Department: Documents: Tacoma Police Using Surveillance Device to Sweep Up Cellphone Data (News Tribune)

WEST VIRGINIA

Police use of cell site simulators unknown

WISCONSIN

Local and state police have cell site simulators

Local Police

- Milwaukee Police Department: "State cops can track residents' cellphones" (Post Crescent)

State Police

- Wisconsin Department of Justice: "State cops can track residents' cellphones" (Gannett Wisconsin)

WYOMING

Police use of cell site simulators unknown

Federal Agencies Known to Use Cell Site Simulators:



**Federal
Bureau of
Investigation**



**Drug
Enforcement
Administration**



**U.S. Secret
Service**



**Immigration
and Customs
Enforcement**



IRS



**U.S.
Marshals
Service**



**Bureau of
Alcohol,
Tobacco,
Firearms,
and
Explosives**

**Internal
Revenue
Service**



U.S. Army



U.S. Navy



**U.S. Marine
Corps**



**U.S. National
Guard**



**U.S. Special
Operations
Command**



**National
Security
Agency**

SIGN UP FOR BREAKING NEWS

GO[PUBLICATIONS](#)[MULTIMEDIA](#)[MEDIA](#)[CONTACT](#)[DONATE](#)

BECAUSE FREEDOM CAN'T PROTECT ITSELF



[USER AGREEMENT](#) | [PRIVACY STATEMENT](#) | [ACCESSIBILITY](#)

This is the website of the American Civil Liberties Union and the American Civil Liberties Union Foundation.

Learn more about these two components of the ACLU.

© 2016 ACLU

The
Intercept

UNOFFICIAL
_SOURCES

FBI Told Cops to Recreate Evidence From Secret Cell-Phone Trackers

Jenna McLaughlin

May 5 2016, 12:11 p.m.



53

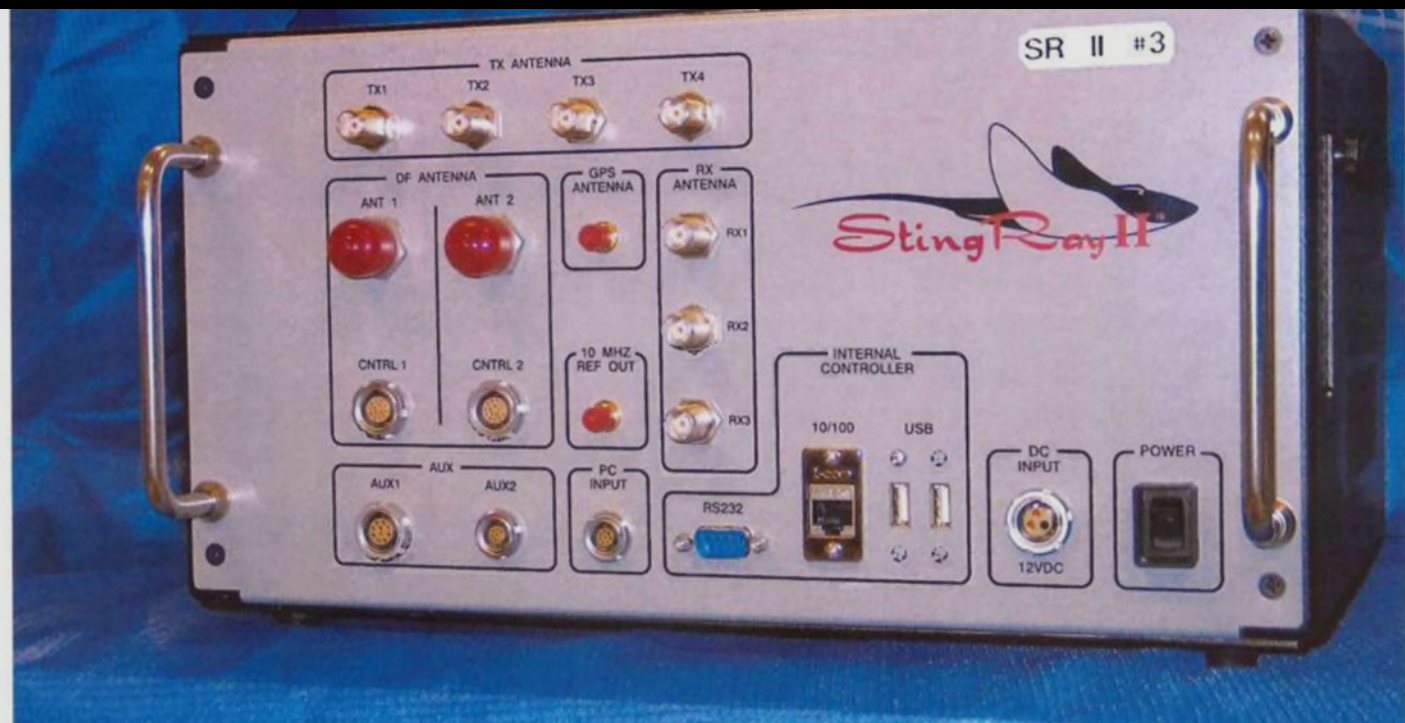


Photo: US Patent and Trademark Office/AP

A RECENTLY DISCLOSED [document](#) shows the FBI telling a local police department that the bureau's

covert cell-phone tracking equipment is so secret that any evidence acquired through its use needs to be recreated in some other way before being introduced at trial.

“Information obtained through the use of the equipment is FOR LEAD PURPOSES ONLY,” FBI special agent James E. Finch wrote to Chief Bill Citty of the Oklahoma City Police Department.

The official notice, dated September 2014, said such information “may not be used as primary evidence in any affidavits, hearings or trials. This equipment provides general location information about a cellular device, and your agency understands it is required to use additional and independent investigative means and methods, such as historical cellular analysis, that would be admissible at trial to corroborate information concerning the location of the target obtained through the use of this equipment.”

The document, [obtained by](#) nonprofit investigative journalism outlet Oklahoma Watch, pertains to the use of cell site simulators, or Stingrays — surveillance technology that mimics a cellphone tower to trick cellphones into transmitting location data and other information, sometimes even the contents of calls.

Journalists and activists have uncovered at least 20 similar nondisclosure agreements between FBI and local police about Stingrays in the past few [years](#) —

but the FBI's advice about retroactively recreating evidence appears to be new.

Privacy advocates have long warned of “parallel construction,” in which investigators cover up information obtained without a warrant by finding other ways to attribute it – never allowing the source of the original lead to be scrutinized or subject to judicial oversight.

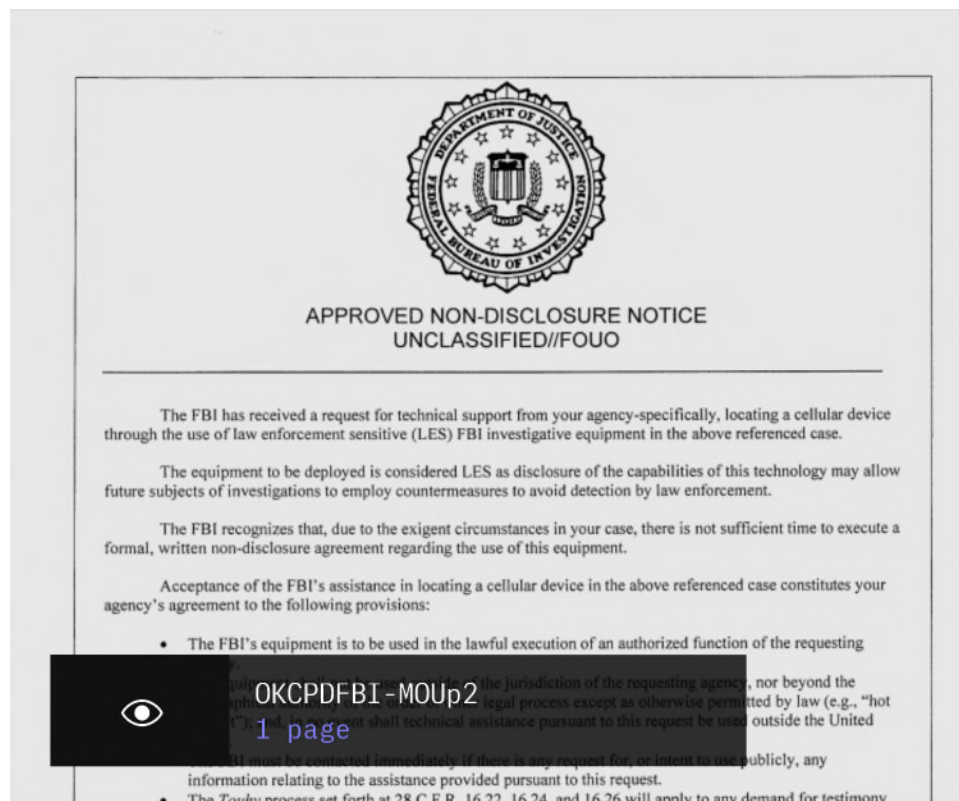
“This is the first time I have seen language this explicit in an FBI non-disclosure agreement,” Nate Wessler, a staff attorney with the American Civil Liberties Union’s Speech, Privacy, and Technology Project, wrote in an email to *The Intercept*. “The typical NDAs order local police to hide information from courts and defense attorneys, which is bad enough, but this goes the outrageous extra step of ordering police to actually engage in evidence laundering,”

“Instead of just hiding the surveillance, the FBI is mandating manufacture of a whole new chain of evidence to throw defense attorneys and judges off the scent. As a result, defendants are denied their right to challenge potentially unconstitutional surveillance and courts are deprived of an opportunity to curb law enforcement abuses,” Wessler continued.

One [concrete](#) example of law enforcement engaging in parallel construction was the Drug Enforcement Agency’s “Hemisphere” program, in which agents

were given access to troves of AT&T's historical cell phone records and instructed to subpoena those same records to create a separate legitimate evidence trail.

Read the rest of the notice here:



Related:

- [FBI Chooses Secrecy Over Locking Up Criminals](#)
- [How the NSA Built Its Own Secret Google](#)
- [The Secret Surveillance Catalogue](#)



CONTACT THE AUTHOR:



Jenna McLaughlin

✉ jenna.mclaughlin@theintercept.com



@JennaMC_Laugh



53 Comments (closed)

The
Intercept_

Newsletter

Don't miss the best of The Intercept

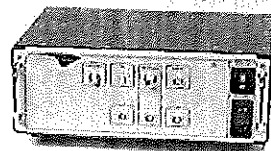
Enter your email address

Email list managed by MailChimp

Stingray phone tracker

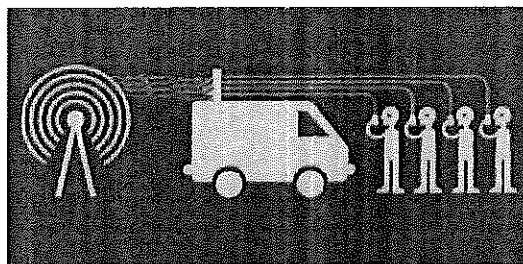
From Wikipedia, the free encyclopedia

The **StingRay** is an IMSI-catcher, a controversial cellular phone surveillance device, manufactured by Harris Corporation.^[2] Initially developed for the military and intelligence community, the StingRay and similar Harris devices are in widespread use by local and state law enforcement agencies across the United States^{[3][4]} and possibly covertly in the United Kingdom.^[5] **Stingray** has also become a generic name to describe these kinds of devices.^[6]



A Stingray device in 2013, in Harris's trademark submission.^[1]

The StingRay is an IMSI-catcher with both passive (digital analyzer) and active (cell site simulator) capabilities.



When operating in active mode, the Stingray device mimics a wireless carrier cell tower in order to force all nearby mobile phones and other cellular data devices to connect to it.