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

Available at: https://works.bepress.com/marc_jonathan_blitz/15/
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 Katz Revolution: Strengthening and Expanding the Protection of Private Spaces ................................................................................ 1366
II. The Technological Challenge to Katz: 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. Tracking ................................................................................................ 1384
      2. Magnification ...................................................................................... 1389
      3. Biometrics and Face Recognition ...................................................... 1390
   C. Detection .................................................................................................. 1398
III. Beyond the Katz 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 Katz 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. Warrant Substitutes and Minimization .............................................. 1457
      2. Selective Warrants ......................................................................... 1464
      3. Unmonitored Recording and Carefully-Restricted Viewing ......... 1467
Conclusion ........................................................................................................... 1479

Introduction

In Lewis Padgett’s 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.” 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. 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. 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].” When curious about the experiences that have shaped him, they can instantly transport themselves back into his childhood. 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.”

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.
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,\textsuperscript{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.”\textsuperscript{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.\textsuperscript{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.\textsuperscript{11} A massive video surveillance system also watches the interior of the city.\textsuperscript{12} Other British cities—according to one

\textsuperscript{8} GEORGE ORWELL, 1984 (1949). “George Orwell” was the pseudonym used by the English novelist and essayist Eric Blair.

\textsuperscript{9} Padgett, supra note 2, at 106.

\textsuperscript{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.


\textsuperscript{12} MCCAHILL & 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 all—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, many “indistinguishable from lampposts,” sit above parks and streets throughout the city and on the campuses of schools and universities. The City of Baltimore has installed cameras at “all 106 downtown intersections” and in its Inner Harbor area. 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. Chicago has recently joined the list of major cities installing cameras over public streets, and other American cities are doing so as well.

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. They can isolate an individual in a business district or subway station, zoom in on

---

13. Rosen, supra note 11, at 41.
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).
him, and scrutinize facial expressions, movements, even reading materials in close detail. 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. 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.

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.” 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.

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 IMAGING, 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.


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. 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. But technological developments are rapidly transforming camera systems and facial recognition devices into far more powerful instruments than they once were. 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.”


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.” 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.” 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. 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.

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 movement 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.

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.”

---

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., Caldorola 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. 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. 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." 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." 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." 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.

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

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.
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.\footnote{34.2} 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.”\footnote{34.3} 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.”\footnote{34.4}

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

\footnote{34.2} New Jersey v. T.L.O., 469 U.S. 325, 333 (1985).
\footnote{34.3} 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.
\footnote{34.4} 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 1960s and are becoming more prevalent, federal courts have yet to seriously address the question of how to analyze them under the Fourth Amendment.

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. The Fourth Amendment does not bar all warrantless searches; it bars only those that are unreasonable. 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. 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). 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.
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.\textsuperscript{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.\textsuperscript{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."\textsuperscript{54} For example, "fires and epidemics [that] ravage large urban areas,"\textsuperscript{55} train wrecks that cause "great human loss,"\textsuperscript{56} and plane hijackings that claim "hundreds of human lives"\textsuperscript{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,\textsuperscript{58} periodic and limited housing inspections,\textsuperscript{59} and brief alcohol and drug tests aimed exclusively at train operators or other employees whose jobs had potentially significant implications for public safety.\textsuperscript{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

\textsuperscript{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. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 10.6 (3d ed. 1996) (outlining the history and legal implications of airport searches).

\textsuperscript{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).


\textsuperscript{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)).

\textsuperscript{58} Id. at 501–02.

\textsuperscript{59} Camara, 387 U.S. at 535.

\textsuperscript{60} Skinner, 489 U.S. at 628.
portion of our day-to-day existence, but instead permeates the whole of public life. 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; that scuba-diving terrorists might sabotage boats or strike coastal areas; that attackers might use trucks or other vehicles as weapons on public roadways; and that they might poison water supplies, target large holiday gatherings and national monuments, shoot down airplanes with missiles, or use explosives, chemical weapons or radiological bombs to kill thousands in subways or town centers. 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).


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).


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 “‘in 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.


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."

After all, one of the key arguments against extending constitutional limits to public camera systems is that the sidewalks, parks, and plazas that these cameras watch over are not private places like the home. 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. 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." The Fourth Amendment, one might say, protects privacy anywhere that people reasonably expect to have such privacy. Since people reasonably expect to be free from ongoing government surveillance even on sidewalks, plazas, and parks, the Fourth Amendment should have force in

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, arc 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."\(^8\)

Christopher Slobogin has likewise built a compelling case for constitutional restriction of public video surveillance by "ta[k]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.'"\(^8\)

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

---

\(^8\) 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-0/opinion_020410_e.asp.

\(^8\) 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," 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) 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

---

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.

I. 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" 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."  

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."  

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. 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. 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. "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. 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." 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." 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." It would be perverse, the Court emphasized, to place any constitu-

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).
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 remedy 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. 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). In *United States v. Karo,* for example, the Court barred the government from using a beeper to track a defendant inside his house. 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. 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.”

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.” Moreover, as David Sklansky has emphasized, in the modern world, such “constitutionally

---

103. *Id.* at 159–60.
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. 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, Justice Harlan tried in Katz to preserve but modernize the notion of specific enclaves where Fourth Amendment privacy protections have especially strong force.

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. 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.\textsuperscript{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 \textit{Katz} when analyzing video surveillance: “A person has a ‘halo’ of privacy \textit{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...”\textsuperscript{113} As noted earlier, \textit{Katz} itself made clear that its goal was to extend Fourth Amendment privacy rights beyond those particular zones or sites traditionally regarded as “private.”\textsuperscript{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.”\textsuperscript{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 \textit{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.\textsuperscript{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 \textit{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.\textsuperscript{117} But it did not clearly define how one might do so other than by

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{112} See \textit{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.”).
\item \textsuperscript{113} State v. Bonnell, 856 P.2d 1265, 1275 (Haw. 1993) (internal quotations and citations omitted) (emphasis added).
\item \textsuperscript{114} \textit{Katz}, 389 U.S. at 350–53.
\item \textsuperscript{115} \textit{Id.} at 351.
\item \textsuperscript{116} William C. Heffernan, \textit{Fourth Amendment Privacy Interests}, 92 J. CRIM. L. & CRIMINOLOGY 1, 59 (2001).
\item \textsuperscript{117} \textit{Katz}, 389 U.S. at 351.
\end{itemize}
\end{footnotesize}
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. Taborda,\(^{125}\) 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. This doctrine, adopted by the Court in 1924, provides that the protection of the Fourth Amendment “is not extended to the open fields.” 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.’” 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*. 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*.” 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

---

130. *Oliver*, 466 U.S. at 179.
131. See infra subpart III(B).
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. 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." 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. 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.

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.\footnote{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”).}

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”).\footnote{As science fiction writer William Gibson recently noted of such technological transformations, “the street itself seem[s] to have evolved” into a “sensory apparatus.”}

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

\footnote{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, \textit{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, \textit{supra} note 27, at 72.}

\footnote{See Jeffrey Rosen, \textit{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”).}

\footnote{William Gibson, \textit{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

---


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. 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.”

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. 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.” 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.
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. 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. 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. 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.

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” and demanded extensive justification from government agents who had used such a surveillance method to monitor the interior of a private business, 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. 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.” In short, the crucial factor for the Tenth Circuit was whether the surveillance took place “inside” or “outside.” 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,” while the outside surveillance (analyzed in the Tenth Circuit’s Jackson case) was aimed at the area just outside someone’s home.

A similar stance on the constitutionality of public video surveillance has been adopted by virtually every state and federal court to address the issue. 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.”

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

158. Id.
159. Id.
160. Mesa-Rincon, 911 F.2d at 1443.
161. Jackson, 213 F.3d at 1276.
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. 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. “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).

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.” 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.” 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. None of these courts was willing to state that individuals’ right against being videotaped extended to parks and streets as well as office space. 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.”\textsuperscript{171} But while cases such as \textit{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.\textsuperscript{172} While federal and state court cases have been almost unanimous in permitting the government to aim cameras at \textit{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.”\textsuperscript{173} Having denied the defendant Fourth Amendment protection, it hastily added that matters might be different “where video surveillance is \textit{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.”\textsuperscript{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,\textsuperscript{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

\textsuperscript{171} United States v. Gonzalez, 328 F.3d 543, 548 (9th Cir. 2003).
\textsuperscript{172} \textit{E.g.}, State v. Costin, 720 A.2d 866 (Vt. 1998); Cowles v. State, 23 P.3d 1168, 1171 (Alaska 2001).
\textsuperscript{173} \textit{Costin}, 720 A.2d at 869.
\textsuperscript{174} \textit{Id.} at 870 (emphasis added).
\textsuperscript{175} \textit{Cowles}, 23 P.3d at 1171.
reasonable grounds to believe that [the employee] was stealing.'

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. It is, after all, only searches and seizures which must be reasonable under the Fourth Amendment. 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. Miami also experimented with video surveillance in the early 1980s. 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. Recently, the Defense Advanced Research Projects Agency (DARPA) has encouraged development of video technology that can automatically record the

176. Id. at 1175.
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."
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.” 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. 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.” 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.

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. 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,” 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. 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. 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.

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. 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” and can raise no Fourth Amendment objection when police electronically follow or retrace those movements even without a good basis for doing so.

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. To do so, it implied, would confine law enforcement to primitive means for detecting and investigating evidence of crime. 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. 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.”

As the Court hastened to add in Knotts and made even clearer a year later in United States v. Karo, 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. 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.\textsuperscript{199} This, of course, is simply an application of the general principle voiced in Justice Harlan’s \textit{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.”\textsuperscript{200}

This straightforward application of the \textit{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 \textit{mass suspicionless} surveillance,\textsuperscript{201} the Court in \textit{Knotts} stressed that universal, round-the-clock tracking of \textit{many} citizens might well require a different constitutional analysis.\textsuperscript{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.”\textsuperscript{203}

At that time, the Court was able to treat such a warning as nothing more than speculation about an unlikely future.\textsuperscript{204} It noted that “reality hardly suggests” that this kind of dragnet searching was taking place.\textsuperscript{205} As Christopher Slobogin points out, it would be harder for the Court to offer the same response now.\textsuperscript{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.\textsuperscript{207}

\begin{itemize}
\item \textsuperscript{199} \textit{E.g.}, \textit{Karo}, 468 U.S. at 715.
\item \textsuperscript{200} \textit{Katz} v. United States, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring).
\item \textsuperscript{201} \textit{E.g.}, State v. Costin, 720 A.2d 866, 870 (Vt. 1998); Cowles v. State, 23 P.3d 1168, 1175 (Alaska 2001).
\item \textsuperscript{202} See \textit{Knotts}, 460 U.S. at 283–84 (noting that unscrupulous use of twenty-four hour surveillance might implicate different constitutional principles).
\item \textsuperscript{203} \textit{Id.} at 284.
\item \textsuperscript{204} \textit{Id.}
\item \textsuperscript{205} \textit{Id.} at 283.
\item \textsuperscript{206} Slobogin, \textit{supra} note 38, at 215–16.
\item \textsuperscript{207} See 47 C.F.R. §§ 20.3, 20.18 (requiring mobile radio service providers to identify calling parties for 911 systems); \textit{see also}, \textit{e.g.}, Fourth Memorandum Opinion and Order, In the Matter of Revision of the Commission’s Rules To Ensure Compatibility with Enhanced 911 Emergency
\end{itemize}
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,\footnote{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/bandtlezintro.htm (last visited Mar. 17, 2004).} I-Pass in Illinois,\footnote{ISTHA I-Pass, at http://www.illinoistollway.com/ipass/default.asp (last visited Jan. 13, 2004).} and FasTrak in California,\footnote{FasTrak Electronic Toll Collection, at http://www.dot.ca.gov/fastrak (last visited Jan. 13, 2004).} 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.\footnote{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).} 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.”\footnote{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”).} The same technologies that allow lost drivers to find out where they are, what services are nearby, and how to get where they are going\footnote{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.} 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.\footnote{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”).} This has caused worry about whether such technology will make deeper inroads into drivers’ privacy,\footnote{I-Pass Takes a Toll on Crime, MILWAUKEE J. SENTINEL, Oct. 13, 2002, at 24A.} 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.\footnote{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).}
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.\(^2\)\(^1\)\(^6\) Fearful of kidnapping, some people have considered installing trackable computer chips into their own bodies (or those of their children).\(^2\)\(^1\)\(^7\) 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.*\(^2\)\(^1\)\(^8\) 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).


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. 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.

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.” While federal courts have not hesitated to hold that use of a telescope to spy upon activities in the home might constitute a search, the Court stressed this was not the case here.

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

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.
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, and critics point to recent tests showing poor performance in surveillance at airports and other environments.227 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.228 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").
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).
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%).

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. 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.” Although the city recently ended the experiment after finding the technology did not help lead police to criminals, 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. Other states are using facial recognition systems to guard against fraudulent acquisition of drivers licenses. 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.

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.


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. 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. 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." 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."
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” process 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”—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. 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. 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. Indeed, such lightning-fast automated

---

241. This process is normally treated as confidential by the company that produces the biometric process. NANAVATI 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. NANAVATI 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

---

\(^{246}\) 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.”).

\(^{247}\) 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.").


\(^{250}\) *Id.* at 238 n.5, 239.
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.

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..." 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.

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." 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, the three-dimensional geometry of her hand, or the distinctive physical attributes of her eyes, such as the vein patterns in her retinas or the structure of her irises. Without audio capacity, cameras


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

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,

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”); NANAVAL 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).


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 distur-
bances 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 Sentor," 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

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

268. Id. at 10.

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.\textsuperscript{271} Other devices "emit puffs of air that pick particles off [airline travelers'] clothing" for instantaneous chemical analysis,\textsuperscript{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.\textsuperscript{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.\textsuperscript{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:

\begin{quote}
[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
\end{quote}

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{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 Sentry 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." \textit{Id}.
\item \textsuperscript{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, \textit{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"); \textit{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"), \textit{transcript available at http://www.hienergyinc.com/press/CNNFN%20Market%20Call_103002.pdf}.
\end{itemize}
\end{footnotesize}
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 Sentor and other devices, one might argue, fit this description. After

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.”).
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.
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. 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. 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.

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. 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.

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. 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

286. Id. at 109–10.
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.").
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 sniffee."\(^{295}\) 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.

---

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.\(^8\) 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*.\(^9\) If, as the Supreme Court held in *Knotts*, a single individual has no reasonable expectation that his movements will remain shielded from intensive scrutiny,\(^6\) 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

\(^9\) See supra notes 269–70 and accompanying text.

\(^6\) 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).

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. 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." 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." 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


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. 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.

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


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.\textsuperscript{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 \textit{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.”\textsuperscript{308} In \textit{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.”\textsuperscript{309} Most recently, in \textit{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.\textsuperscript{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,”\textsuperscript{311} it would be odd if new

\textsuperscript{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, \textit{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 \textit{id.} at 581–90; see also Rodney A. Smolla, \textit{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”).

\textsuperscript{308} 357 U.S. 449, 462 (1958).


\textsuperscript{310} 536 U.S. 150, 166–69 (2002).

\textsuperscript{311} United States v. Cusamano, 83 F.3d 1247, 1265 (10th Cir. 1996) (finding, as the Supreme Court later did in \textit{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.  

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.” 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. 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].”

For all of these reasons, 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.


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.” 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. 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, 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).


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.”\(^\text{320}\) Even after *Olmstead* was overruled by *Katz*, the Court again expressed the concern, in *Ciraolo*,\(^\text{321}\) 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.”\(^\text{322}\) 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.\(^\text{323}\) 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


\(^{322}\) *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,

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.\(^\text{327}\)

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."\(^\text{328}\)

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 peeking 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.\(^\text{329}\)

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.\(^\text{330}\) Thus, while people might be horrified

\(^{327}\) As Justice Scalia made clear in \textit{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 . . . \textit{all} details are intimate details, because the entire area is held safe from prying government eyes." \textit{Kyllo}, 533 U.S. at 37.

\(^{328}\) See Heffernan, \textit{supra} note 116, at 36–37.


\(^{330}\) Heffernan, \textit{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.\textsuperscript{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.\textsuperscript{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 untrammeled video surveil-
lance of streets and other public spaces.\textsuperscript{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.”\textsuperscript{334} By
contrast, a hidden watcher at a monitor is “unchecked” by norms of social
interaction.\textsuperscript{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

\begin{itemize}
\item \textsuperscript{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 Hefferman, 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).
\item \textsuperscript{332} See Hefferman, 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”).
\item \textsuperscript{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”).
\item \textsuperscript{334} Jennifer Mulhem Granholm, Video Surveillance on Public Streets: The Constitutionality of
\item \textsuperscript{335} Id.
\end{itemize}
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. 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.” Lessig and other privacy law scholars, such as Joel Reidenberg and Daniel Solove,

---

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.

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.”

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, 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


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

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." 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.

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. 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.”

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

“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. They should examine instead “the nature of a particular practice and the likely extent of its impact on the individual’s sense of security.” 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. 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.”

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.

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.” 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

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.
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, 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.

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.” 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, 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.\textsuperscript{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 \textit{Roe v. Wade}\textsuperscript{\textit{361}} and \textit{Griswold v. Connecticut}\textsuperscript{\textit{362}} and they have arguably done so in holding, in the case of \textit{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."\textsuperscript{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

\textsuperscript{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, \textit{Privacy's Problem and the Law of Criminal Procedure}, 93 MICH. L. REV. 1016, 1046 (1995).

\textsuperscript{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).

\textsuperscript{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").

\textsuperscript{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. 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.

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.\textsuperscript{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 \textit{djinn cannot be crammed back into its bottle.}\textsuperscript{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."\textsuperscript{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.\textsuperscript{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.\textsuperscript{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

\textsuperscript{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 \textit{per se} is justified by a reasonable governmental interest in protecting national air commerce.").

\textsuperscript{370} \textit{BRIN, supra} note 16, at 8.

\textsuperscript{371} \textit{Id.} at 9.

\textsuperscript{372} \textit{Id.} at 23.

\textsuperscript{373} \textit{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.  

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.

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. 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. 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. 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. 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. 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).

treat, 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. 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. 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

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

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

---


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, various commentators 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."

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

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").
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.” 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.” Another court was likewise “willing to assume arguendo that the appellants, as they profess, had some subjective expectation of privacy while at work,” 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.”

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, 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.
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.\footnote{A number of writers emphasize that the nature of privacy shifts as society changes. \textit{E.g.}, \textit{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, \textit{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 (\textit{e.g.}, gold) beyond those which we currently recognize with our senses (\textit{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. \textit{See JOHN LOCKE, AN ESSAY CONCERNING HUMAN UNDERSTANDING}, bk. II, ch. XXIII, §§ 10–12, at 301–03 (Peter H. Nidditch ed., Oxford Univ. Press 1975) (1690).}

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.\footnote{Adler, \textit{supra} note 288, at 1111–12.} 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
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." 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]." 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. 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).
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.\footnote{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.\footnote{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,\footnote{410} these are hardly realistic proposals for shielding one's day-to-day activities.\footnote{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."\footnote{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.\footnote{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.

\footnote{408} Id. He mentions only "the place observed" and "minimization" as "central to any analysis of physical surveillance technology." Id. at 398.

\footnote{409} Id. at 398–401.

\footnote{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").

\footnote{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.

\footnote{412} See Slobogin, supra note 325, at 400.

\footnote{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.” 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.”

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.

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.” 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.”

As noted earlier, the Court’s wiretap analysis in Berger already required “minimization” as a condition of a warrant, 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.

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.
417. Id. at 238 & n.5.
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 LaFave 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.\textsuperscript{424} In a similar vein, David Sklansky argues that
the key lesson that the current Court should distill from \textit{Katz} is that “the
privacy protected in \textit{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.”\textsuperscript{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 \textit{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.”\textsuperscript{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.\textsuperscript{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

\begin{footnote}
\textsuperscript{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.”).

\textsuperscript{425} Sklansky, supra note 102, at 195.

\textsuperscript{426} 923 F.2d 665, 677 (9th Cir. 1991); see also cases discussed supra subpart II(A).

\textsuperscript{427} As noted in subpart II(A), the Ninth Circuit, despite its \textit{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 \textit{Knotts} imposed no constitutional limits on
how closely police might track individuals on public roadways. \textit{United States v. Knotts}, 460 U.S.
\end{footnote}
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* and the kind of identity-revealing magnification that troubled the Court in *Dow Chemical* 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.”

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.” 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.” Rather, he noted, this question can be answered only if it is “transmuted” into a framework that is more administrable. 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. But “reasonable expectations of privacy” are also difficult for judges...
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

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*. 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.” 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, 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.” 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.” 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

---

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).
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. Place447 and United States v. Jacobsen448 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).


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. 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. 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.

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.” The Supreme Court has stated that warrantless searches are justifiable, for example, to prevent train wrecks that cause “great human loss” or to address health epidemics. It has allowed warrantless searches at the national border, where security is a significant concern, 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, 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).


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.”).

searches are needed to serve “special needs, beyond the normal need for law enforcement.”

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.”

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.”

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 airports and federal buildings. Although some courts have said that such programs are designed simply to protect the safety of air travelers, it seems disingenuous
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.\footnote{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 \textit{Skinner, Von Raab}, and \textit{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.\footnote{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.\footnote{470}

\footnote{468. For this reason, subsequent courts have rejected the Ninth Circuit’s statement in \textit{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.” \textit{United States v. Herzbrun}, 723 F.2d 773, 776 (11th Cir. 1984). Even the Ninth Circuit itself has reconsidered and limited \textit{Davis’s} holding, allowing exit only before a passenger places his bags on an x-ray belt. \textit{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.”).}

\footnote{469. \textit{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.”); \textit{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.”); \textit{Vernonia Sch. Dist. 471 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.”).}

\footnote{470. \textit{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. 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.

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.” Gaiioni 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.\textsuperscript{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.\textsuperscript{475} It is also in accord with the sentiments,

\textsuperscript{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 \textit{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,” \textit{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.” \textit{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.” \textit{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,” \textit{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 \textit{Zurcher v. Stanford Daily}.

\textsuperscript{475} See, e.g., Gary Langer, \textit{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.\textsuperscript{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,\textsuperscript{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.\textsuperscript{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."\textsuperscript{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


\textsuperscript{477} Olmstead v. United States, 277 U.S. 438, 472–73 (1928) (Brandeis, J., dissenting).

\textsuperscript{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.

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 cases—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/ar-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.” 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.” 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:

(1) They leave the searching official with little discretion because of the standardization in:

   (a) the purposes for which the search will be administered;

   (b) how the search is conducted; and

---


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.\textsuperscript{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;\textsuperscript{487}

(b) are often entirely avoidable;\textsuperscript{488}

(c) reveal little information—often only the presence or absence of drugs or metallic objects;\textsuperscript{489} and

(d) occur against the backdrop of regulated environments—leaving freer environments relatively untouched.\textsuperscript{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;\textsuperscript{491} and

(b) the type of search used is well-suited to address this problem.\textsuperscript{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

\textsuperscript{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").

\textsuperscript{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 . . . .").

\textsuperscript{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).

\textsuperscript{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").

\textsuperscript{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.").

\textsuperscript{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).

\textsuperscript{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").

\textsuperscript{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).
To guard against this possibility, the Court insisted that warrantless roadblock examinations could be used only for certain "programmatic 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.
searches of everyone who has a need to travel. 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.

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, 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. 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.

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. 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.
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.

HeinOnline -- 82 Tex. L. Rev. 1460 2003-20042
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).


510. Id. at 41.
undesirable effect on crime.\textsuperscript{511} The reduction in crime was even more negligible—only two percent—in downtown areas, where many cities are placing cameras.\textsuperscript{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.\textsuperscript{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

\textsuperscript{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”).

\textsuperscript{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.

\textsuperscript{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, 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 iden-
tify 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 govern-
ment 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. 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).
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.\textsuperscript{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,\textsuperscript{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.”\textsuperscript{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.”\textsuperscript{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.\textsuperscript{520}

In a similar vein, members of legislatures in two states, Virginia and California, have considered requiring warrants for police use of facial

\textsuperscript{516} See supra subpart II(A).
\textsuperscript{518} Id. § 6(a), (c).
\textsuperscript{519} Id. § 13(c).
\textsuperscript{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, but this warrant requirement was ultimately eliminated from the bill. 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. 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. 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." 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. Some might argue that such a requirement would undercut governments' efforts to locate suspected terrorists with no criminal record. 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.

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.").
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 underruns 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/ls/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." 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. As James Carr and Patricia Bellia have noted in the contexts of communications interception, "[p]articularization 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.

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.
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.”

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. 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. 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, 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).
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.\textsuperscript{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.\textsuperscript{538} As Justice Marshall pointed out in his dissent in \textit{Skinner}, the urinalysis drug testing conducted by the government really involved multiple searches, not just one.\textsuperscript{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.\textsuperscript{540}

\textsuperscript{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, \textit{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." \textit{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." \textit{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.


\textsuperscript{539} \textit{Id.} at 642 (Marshall, J., dissenting).

\textsuperscript{540} \textit{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.” 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.”

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.

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")


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.”\textsuperscript{544} In \textit{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.”\textsuperscript{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 \textit{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.\textsuperscript{546} In \textit{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.\textsuperscript{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 \textit{Earls}. Thus courts might ensure that the data is encrypted and perhaps protected with passwords

\textsuperscript{544} 536 U.S. 822, 833 (2002).
\textsuperscript{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. \textit{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”).
\textsuperscript{546} \textit{Earls}, 536 U.S. at 833.
\textsuperscript{547} 515 U.S. 646, 660 (1995).
Video Surveillance and the Constitution of Public Space

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. 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, 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”).

purged instantly.\textsuperscript{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.\textsuperscript{552} In cyberspace, for example, people might distinguish themselves from others only with an e-mail address or username.\textsuperscript{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.\textsuperscript{554} But even in law enforcement, it

\textsuperscript{551} Mark G. Milone, Biometric Surveillance: Searching for Identity, 57 BUS. L.\textit{\textsuperscript{A}}.W. 497, 509–11 (2001) (citing "responsible use principles" proposed by Visionics, a manufacturer of facial recognition software).

\textsuperscript{552} \textsc{NANAVATI ET AL.}, supra note 226, at 10–11.

\textsuperscript{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." \textsc{Lessig}, \textit{supra} note 101, at 33.

\textsuperscript{554} \textit{See, e.g.,} Clymer, \textit{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.\textsuperscript{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."\textsuperscript{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 measurements\textsuperscript{557}—for the same reason that one cannot reconstruct a 400-page novel from an identifying record which samples every 20th letter.\textsuperscript{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 cameras. 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

\textsuperscript{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).

\textsuperscript{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.").

\textsuperscript{557} NANAVATI ET AL., supra note 226, at 13.

\textsuperscript{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.”

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.

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. He took note of recent technological advances and of the opportunities they created for “[s]ubtler and more far-reaching means of invading privacy.”

“Can it be,” asked Brandeis of the new forms of surveillance, “that the Constitution affords no protection against such invasions of individual security?”

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. 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, keep drunk drivers off the highways, or address drug epidemics. 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.

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
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, 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.”

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).

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.