

The Case for Stewart over Harlan on 24/7 Physical Surveillance

Afsheen John Radsan^{*}

I. Introduction

My premise is that the government's physical surveillance can reach a point in terms of duration and intensity that it becomes a "search" under the Fourth Amendment. If one accepts the common sense of this premise, the law of surveillance should change. The changes can come from the Executive branch by orders, regulations, or guidelines; from Congress by a statute that gives citizens more protections from governmental intrusions than the courts have given so far; or from the courts by new holdings that do a better job of balancing individual freedom against the government's duty to protect us from dangers, including terrorist attacks.

If, by doctrinal change, some types of physical surveillance are accepted as a search, subsidiary questions present themselves. Is a warrant required? Probable cause? Reasonable suspicion? Or is an even lower standard possible that recognizes that terrorism cases are significantly different from ordinary cases? If individual suspicion is not there, the government might attempt to justify a search through some "special need." But arguing for a special need (say, in a sobriety checkpoint) is quite different in doctrinal terms from arguing that a search did not occur at all (say, in a canine sniff of a piece of luggage).¹ This Article, while not indifferent to these subsidiary questions, does not specify the appropriate level of suspicion for pervasive, physical surveillance. Nor does it apply the proposed framework to rework all Supreme Court cases since 1967 on what constitutes a search. Instead, this Article examines just one area of Fourth Amendment jurisprudence through the dark lens of 9/11.

In helping to answer when governmental action becomes a search, *Katz v. United States*² and *Kyllo v. United States*³ stand out from the canon. Depending on one's point of view, *Kyllo* may be the last case from the *Katz* era

^{*} Professor of Law, William Mitchell College of Law. Professor Radsan is a former federal prosecutor. He thanks Adam Pabarcus, Christopher Proczko, and Dan Ryan for their outstanding research assistance.

1. Compare Andrea J. Cook, *Sobriety Checkpoints Deter Drunken Drivers*, RAPID CITY J., Mar. 15, 2010, available at http://www.rapidcityjournal.com/news/article_02ab6a3c-2fdc-11df-b99d-001cc4c03286.html (discussing the implementation and effectiveness of sobriety checkpoints), with David G. Savage, *High Court to Rule on 'Canine Sniff' Search*, L.A. TIMES, Apr. 6, 2004, available at <http://articles.latimes.com/2004/apr/06/nation/na-scotus6> (discussing a case in which prosecutors argued that a dog sniffing the air does not amount to a search).

2. 389 U.S. 347 (1967).

3. 533 U.S. 27 (2001).

or the first case from a new era. *Katz*, decided in 1967, swept away a prior emphasis on property rights and trespass laws to hold that the electronic monitoring of a phone booth was a search.⁴ Since then, the two-part test from Justice Harlan's concurring opinion has received as much attention as the totality-of-the-circumstances test in Justice Stewart's majority opinion.⁵ *Kyllo*, decided just months before 9/11, ruled that the government's use of a thermal-imaging device from outside a house was a search.⁶ For the era after 9/11, a blend of Justice Harlan's test in *Katz* with Justice Scalia's opinion in *Kyllo* reproduces Justice Stewart's test, a more open-ended test which makes room for property, liberty, secrecy, anonymity, autonomy, and privacy, as well as other values that may undergird the "right of the people to be secure in their persons, houses, papers, and effects."⁷ Justice Stewart's test helps not only on one issue of physical surveillance but also opens up new approaches to data mining and other Fourth Amendment issues at the intersection of national security, privacy, and technology.

II. Implications of Another Terrorist Attack

Before the next terrorist attack—and the ensuing panic that will make civil-libertarian proposals even more difficult to achieve⁸—I challenge the consensus that all physical surveillance falls outside the Fourth Amendment.⁹ For these purposes, I limit my analysis to trends in the courts and in academic commentary since 9/11. A sympathetic reader might accept this limitation for at least two reasons. First, the space for a symposium piece does not permit an extensive review of related Fourth Amendment topics:

4. See *Katz*, 389 U.S. at 353 (holding that electronic monitoring of a telephone booth violated the Fourth Amendment, despite the lack of physical intrusion into the booth).

5. See, e.g., Clark D. Cunningham, *A Linguistic Analysis of the Meanings of "Search" in the Fourth Amendment: A Search for Common Sense*, 73 IOWA L. REV. 541, 568 (1988) (noting that the result in *Katz* derived from Harlan's concurrence is "universally praised while the majority opinion either is ignored or deprecated").

6. *Kyllo*, 533 U.S. at 34 ("[O]btaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area,' constitutes a search—at least where (as here) the technology in question is not in general public use." (quoting *Silverman v. United States*, 365 U.S. 505, 512 (1961))).

7. U.S. CONST. amend. IV. See generally Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757 (1994) (arguing that Fourth Amendment searches should be judged not by the Supreme Court's confused and confusing doctrine but by their reasonableness).

8. See, e.g., BRUCE ACKERMAN, *BEFORE THE NEXT ATTACK 2* (2006) (predicting that successful terrorist attacks will result in a proliferation of repressive laws undercutting civil liberties).

9. See Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 381 (1974) (explaining that the "maxim that the eye or ear could not commit a search" traces "back to English common law and had been mentioned by Lord Camden in his celebrated judgment in *Entick v. Carrington*, which has always been justly received as something of a lexicon of the 'original understanding' of the fourth amendment.").

open fields,¹⁰ curtilage,¹¹ garbage bags,¹² pen registers,¹³ and dog sniffs.¹⁴ Second, any conclusions from before 9/11 may not properly factor into the equation the very real possibility of the next catastrophic attack; 9/11, a dividing line between eras, continues as a major marker in policy making and legal analysis.

Definitions are important. My use of the term “physical surveillance” attempts to separate this analysis from an analysis of “electronic surveillance.” The attempted distinction is between FBI agents on the street and National Security Agency computers that suck in e-mail, telephone, and other signals. But physical surveillance is also a bit of a misnomer. FBI agents do not usually seek to make physical contact with their suspects during surveillance; in many cases, the FBI does not want the suspects to know they are being observed.¹⁵ Watching from the shadows, the FBI hopes suspected bad guys will take the FBI to other bad guys.¹⁶ So this sort of surveillance might also be called “visual surveillance.”

Imagine teams of FBI agents following a suspected terrorist in New York City. A team in the lobby across the street watches the suspect leave his apartment on the Upper West Side. They take photographs. Another team joins him on the Number One subway headed downtown. Several teams watch the entrances to 125 Broad Street, the downtown building where the suspect has an office. They use binoculars. Hours go by. Another team tails the suspect by car as he rides out of the garage, driven by another person toward Newark. Helicopters and planes assist the agents on the ground. A command post at FBI headquarters guides their action. Although the agents do not develop enough information for an arrest, they continue to be

10. See, e.g., David E. Steinberg, *The Original Understanding of Unreasonable Searches and Seizures*, 56 FLA. L. REV. 1051, 1058–59 (2004) (discussing the Supreme Court’s holding that the Fourth Amendment does not apply to police searches in open fields).

11. See, e.g., Catherine Hancock, *Justice Powell’s Garden: The Ciraolo Dissent and Fourth Amendment Protection for Curtilage-Home Privacy*, 44 SAN DIEGO L. REV. 551, 559–65 (2007) (describing the Supreme Court’s treatment in *Ciraolo* of pre-*Katz* curtilage doctrines).

12. See, e.g., Brian J. Serr, *Great Expectations of Privacy: A New Model for Fourth Amendment Protection*, 73 MINN. L. REV. 583, 616–24 (1989) (discussing the Supreme Court’s holding in *California v. Greenwood*, 486 U.S. 35 (1988), that property owners have no subjective expectation of privacy in their garbage that society would accept as “objectively reasonable”).

13. See, e.g., Paul M. Schwartz, *Warrantless Wiretapping, FISA Reform, and the Lessons of Public Liberty: A Comment on Holmes’s Jorde Lecture*, 97 CAL. L. REV. 407, 427–28 (2009) (lamenting the lack of pen-register reports by Congress as authorized by the Pen Register Act).

14. See Savage, *supra* note 1 (discussing a case in which prosecutors argued that a dog sniffing the air does not amount to a search).

15. See *Weekend Edition Saturday: FBI Surveillance Team Reveals Tricks of the Trade* (NPR radio broadcast July 5, 2008), available at <http://www.npr.org/templates/transcript/transcript.php?storyId=92207687> (describing a variety of FBI surveillance techniques designed to ensure that suspects are unaware of the FBI’s presence).

16. See *Talk of the Nation: How to Prevent Home Grown Terrorism* (NPR radio broadcast Dec. 15, 2009), available at <http://www.npr.org/templates/story/story.php?storyId=121473067> (proclaiming that one of the main goals of surveillance is to find other people to further the investigation).

suspicious based on their read of the suspect and on tips from the Intelligence Community. The FBI is not allowed to use these tips in a search warrant, however, because the Intelligence Community insists on full protection for its sources and methods as the price for its cooperation on this case. Not sure what else to do, the FBI adds teams and resources. In early September, the suspect, backing up on the sidewalk and looking into shop windows on Columbus Avenue, spots the surveillance. The original operation is blown.

Next, as a sort of deterrence, the FBI agents decide to make the surveillance even more visible to the suspect. Everywhere the suspect goes, he knows he is being watched: at home, at work, and in the coffee shop where he smokes a water pipe with friends. His family and friends also see that he is being watched. The surveillance goes on for months. It is expensive—and often boring for the agents. If the law made sense then this sort of open, pervasive physical surveillance would fall under the Fourth Amendment.¹⁷ Unfortunately for the suspect, Fourth Amendment law is not always rational. And the line between investigation and harassment is not always clear.

Terrorism investigations can go from boring to exciting in the click of a trigger. Imagine that the suspect eludes FBI surveillance, and on September 12, 2011, a synchronized set of bombings goes off around the United States. From 8:00 a.m. until 8:30 a.m., in fifteen-minute intervals, the New York subway system, the Washington, D.C. Metro, and the Chicago L are all attacked. The timing and sophistication of the attacks carry al Qaeda's evil signs. The bombs, detonated by cell phones, were contained in backpacks left on the trains. Hundreds are dead, thousands wounded. Panic has set in, and the American public wants the government to do what is necessary for them to feel safe again. In response, government agents are everywhere. The physical surveillance is more intense than after 9/11. The agents on the streets of American cities look like soldiers on battlefields in Afghanistan. They carry machine guns and wear pistols in holsters. On their helmets are swiveling cameras that feed into an elaborate closed-circuit television system; controllers in the FBI's operations center can thus see the scene from the agents' perspectives. The agents see the world through specialized goggles, even more advanced than the infrared devices used by soldiers in Afghanistan. The new goggles, more penetrating than the scanners in security lines at American airports, allow the agents to see through people's clothes and skin for signs of hidden weapons. The frantic agents fear something much worse than the initial attack. With hand-held radiation detectors, far more sophisticated than Geiger counters from days gone by,

17. The text of the Amendment does not limit its application to clandestine searches and seizures. *See* U.S. CONST. amend. IV (preventing the government from violating the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures").

they look for signs that al Qaeda has smuggled a real nuclear weapon into an American city.

Neither this scenario nor the use of technology is far-fetched. Cameras, infrared goggles, and radiation detectors are part of governmental arsenals.¹⁸ These technologies can easily be adjusted and combined for law enforcement purposes.

Across the Atlantic, British residents are accustomed to pervasive CCTV.¹⁹ A ride on a bicycle from Hampstead Heath to Hyde Park is recorded by hundreds, if not thousands, of cameras.²⁰ These cameras feed into command centers around the city.²¹ In this area of government intrusion, the British public seems more resigned than the American public to losses in their privacy. Having endured a time of troubles when the IRA regularly bombed targets, the British lost their innocence long before 9/11.²² Thus, Americans may be catching up to their British cousins on CCTV.

On traditional battlefields, the American soldier's use of infrared goggles gives him a distinct advantage over enemies whose gear is less advanced. At times, the American can literally see through walls,²³ and fighting after the sun has set is still possible because he can see through the blackness of night.²⁴ Military technologies, of course, often lead to civilian variations.²⁵

Radiation detectors were visible to some people in American cities after 9/11.²⁶ Whether the American government acknowledged the specifics or not, any driver heading into Washington, D.C., could easily project an official purpose onto the cables and cords strapped down to main roads and attached to black boxes. Many drivers may have assumed the plain vans in

18. See, e.g., Richard A. Serrano, *FBI Monitors for Radiation at Some Mosques*, L.A. TIMES, Dec. 24, 2005, at A16 (asserting that "investigators used special equipment to gauge radiation levels at homes, businesses, warehouses and centers of some Muslim groups").

19. See, e.g., Helen Carter & David Ward, *CCTV Captures a Boy on a Bike—Thirty Seconds Later He Had Killed Rhys Jones*, GUARDIAN, Sept. 27, 2007, <http://www.guardian.co.uk/uk/2007/sep/27/topstories3.ukguns> (describing CCTV's role in a murder investigation in Liverpool and calls to enhance the system).

20. See Louise Osborne, *Hundreds of CCTV Cameras Watch Surrey Boroughs*, GET SURREY, Aug. 24, 2009, http://www.getsurrey.co.uk/news/s/2056165_hundreds_of_cctv_cameras_watch_surrey_boroughs (revealing that one small borough in England added 493 surveillance cameras over a one-year period).

21. See Chiltern Dist. Council, *How Does the CCTV Work?*, http://www.chiltern.gov.uk/site/scripts/documents_info.php?documentID=57&pageNumber=3 ("Specially trained staff monitor the CCTV pictures in a secure control room in High Wycombe.").

22. See STEVE HEWITT, *THE BRITISH WAR ON TERROR 9–28 (2008)* (chronicling the British history with terrorism, focusing on violence with Ireland).

23. See ROBERT L. SNOW, *TECHNOLOGY AND LAW ENFORCEMENT 90 (2007)* ("[S]everal manufacturers have developed portable, handheld devices that can see through . . . walls and detect motion on the other side.").

24. See *id.* (describing a "flashlight that illuminates the area with infrared radiation, allowing police officers with infrared sensing devices to see clearly in darkened areas").

25. See *id.* (noting that local law enforcement now uses sophisticated technology).

26. *Id.* at 68.

traffic contained even more sophisticated devices to detect biological, chemical, and nuclear weapons. As a faithful former public servant, I neither confirm nor deny.

The use of cameras, goggles, and radiation detectors may increase the government's chances of detecting terrorist plots. But, in a sort of boomerang, their pervasive use, much like the national threat levels perpetually at orange and red, may contribute to the fear that is the terrorist's goal. Whether they are used in the nation's counterterrorism arsenal has as much to do with politics as it does with law. The political calculations after the next attack, no doubt, may be much different from the calculations during the long lull in the homeland. Let us hope this lull lasts. And let us put some reasonable rules in place in advance.

III. The Legal Framework of Fourth Amendment Searches

A. *The Supreme Court*

Two Supreme Court cases, *Katz* and *Kyllo*, are important in determining whether simple or sophisticated surveillance constitutes a search. *Katz v. United States*, decided before the age of terror, was an important shift in the Court's analysis of the Fourth Amendment. Justice Stewart, writing for the Court, made clear the Court's rejection of a prior emphasis on physical trespass: "Once this much is acknowledged, and once it is recognized that the Fourth Amendment protects people—and not simply 'areas'—against unreasonable searches and seizures, it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure."²⁷ Justice Stewart decided that the government's listening to and recording of calls in a phone booth was a search that required a judicial warrant, something the government had not obtained.²⁸ He emphasized the importance of a neutral magistrate in authorizing searches as much as the notion that the Fourth Amendment did not always depend on trespass.²⁹ In reaching his conclusion, Justice Stewart did not present a list of factors—or that much analysis: "The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment."³⁰ Thus, the "public" phone booth played an important role in "private" communications. Overall, Justice Stewart tried to distinguish between what a person "knowingly exposes to the public" and what "he seeks to preserve as private."³¹

27. *Katz v. United States*, 389 U.S. 347, 353 (1967).

28. *Id.*

29. *Id.* at 354–55.

30. *Id.* at 353.

31. *Id.* at 351.

Academics and other judges might criticize Justice Stewart for not saying more on what made the government activity in *Katz* a search. Wiser commentators might see that Justice Stewart realized that some concepts such as “beyond a reasonable doubt” or “reasonable care” do not lend themselves to precision. Indeed, the attempt at too much precision or the use of multi-factored tests might actually undercut the conclusion. Much like the time when he knew “obscenity” when he saw it,³² perhaps Justice Stewart just knew a search when he saw it.

Justice Stewart’s rejection of prior cases and his reformulation of the term “search” opened up the Fourth Amendment to electronic surveillance. This decision was part of the package that prodded Congress into regulating electronic surveillance.³³ Title III³⁴ became the reference for law enforcement searches, and the Foreign Intelligence Surveillance Act³⁵ became the reference for national-security searches within the United States.

From *Katz*, Justice Harlan’s concurring opinion is remembered more than Justice Stewart’s opinion for the Court. Justice Harlan questioned whether the distinction between “people” and “places” was very clear.³⁶ Reference to a place is usually necessary, he believed, in determining whether a person has a constitutionally protected expectation of privacy.³⁷ For Justice Harlan, the telephone booth was a “temporarily private place whose momentary occupants’ expectations of freedom from intrusion are recognized as reasonable.”³⁸ So not only did Justice Harlan blur the distinction between people and places, but he also blurred the difference between public and private spaces. More famously, he offered a two-part test in determining whether a governmental search had occurred: “[F]irst that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as ‘reasonable.’”³⁹ This test, as explained below, has found some favor in the

32. *Jacobellis v. Ohio*, 378 U.S. 184, 197 (1964) (Stewart, J., concurring) (“I shall not today attempt further to define the kinds of material I understand to be [hard-core pornography]; and perhaps I could never succeed in intelligibly doing so. But I know it when I see it, and the motion picture involved in this case is not that.”).

33. See Tara Mikkilineni, Note, *Constitutional Default Rules and Interbranch Cooperation*, 82 N.Y.U. L. REV. 1403, 1411 (2007) (asserting that the Court’s decisions in *Katz* and *Berger v. New York*, 388 U.S. 41 (1967), “both led Congress to regulate electronic surveillance out of fear that the Court would otherwise ban the practice outright.”).

34. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, §§ 801–804, 82 Stat. 197 (1968) (codified at 18 U.S.C. §§ 2510–2522 (2006)).

35. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended in scattered titles of U.S.C.).

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

37. *Id.*

38. *Id.*

39. *Id.*

lower courts.⁴⁰ Those who support Justice Harlan do not seem troubled that the second part of his test turns on the malleable term “reasonable.”

In *Kyllo v. United States*, the Supreme Court, in a 5–4 decision, decided that “the use of a thermal-imaging device aimed at a private home from a public street” constituted a search and therefore required a warrant.⁴¹ This case was decided a few months before 9/11, and it is quite possible that the case would have been decided differently if those attacks were factored into the Court’s calculations. For Justice Scalia, it was very important that the governmental activity was connected with the suspect’s home, a place of maximum constitutional protection from “prying government eyes.”⁴² While acknowledging that “visual” or “naked-eye” surveillance is generally not a search, Justice Scalia said *Kyllo* presented the question of “how much technological enhancement of ordinary perception from such a vantage point, if any, is too much.”⁴³ In that regard, both the majority and the dissent in *Kyllo* devoted many more words to describing changes in technology than the *Katz* Court did. *Kyllo* was a decision for the wired age.

Justice Scalia saw the use of “sense-enhancing” technology as a search to the extent it revealed “details of the home that would previously have been unknowable without physical intrusion.”⁴⁴ Part of the pre-*Katz* era’s emphasis on trespass influenced his analysis. Reaching back to the eighteenth century, he noted “[v]isual surveillance was unquestionably lawful because ‘the eye cannot by the laws of England be guilty of a trespass.’”⁴⁵ Having separated Fourth Amendment rights from trespass and property law, the Court still preserved the possibility of “the lawfulness of warrantless visual surveillance of a home.”⁴⁶ Further, Justice Scalia rejected as unworkable any test that would require warrants for technological intrusions of the home only if they would reveal “intimate details.”⁴⁷ Because the sophistication of the technology has “no necessary connection . . . [to] the ‘intimacy’ of the details that it observes,”⁴⁸ such a distinction would give police officers no way “to know in advance whether [the search] is constitutional.”⁴⁹ Moreover, Justice Scalia determined that “[i]n the home . . . *all* details are intimate details.”⁵⁰ No matter how circular the *Katz* test may be, he maintained a bright line of

40. *See infra* section III(B)(1).

41. 533 U.S. 27, 29 (2001).

42. *Id.* at 37.

43. *Id.* at 33.

44. *Id.* at 40.

45. *Id.* at 31–32 (quoting *Boyd v. United States*, 116 U.S. 616, 628 (1886)).

46. *Id.* at 32.

47. *Id.* at 38.

48. *Id.*

49. *Id.* at 39 (emphasis omitted).

50. *Id.* at 37.

Fourth Amendment protection at the entrance of a home.⁵¹ Yet, insofar as his analysis depends on the technology not being in “general public use,”⁵² Justice Scalia’s protection may not be total. As Justice Stevens noted in dissent, “the threat to privacy will grow, rather than recede, as the use of intrusive equipment becomes more readily available.”⁵³

Justice Stevens, writing with ironical relish, accused Justice Scalia of judicial activism in *Kyllo*. Instead of trying “to craft an all-encompassing rule for the future,” Justice Stevens advised the Court “to give legislators an unimpeded opportunity to grapple with these emerging issues rather than to shackle them with prematurely devised constitutional constraints.”⁵⁴ Justice Stevens did not believe the homeowner had a reasonable expectation of privacy in the mere “heat emissions” from his home.⁵⁵ In addition to heat emissions, Justice Stevens listed other things in the “public domain”: traces of smoke, suspicious odors, odorless gases, and airborne particulates.⁵⁶ Presaging the 9/11 era and the possible use of radiation detectors in this Article’s scenario, he also mentioned “radioactive emissions.”⁵⁷ For the most part, Justice Stevens’s argument is good for those who do not want any limits on physical surveillance. Because this sort of surveillance does not violate a reasonable expectation of privacy, Justice Stevens does not construe it as a search.⁵⁸ Government agents, for him, are free to observe people from places outside their homes.

Other than passing references from Supreme Court justices,⁵⁹ not much case law examines the limits of physical surveillance, before or after 9/11.⁶⁰ The subjects of the surveillance may not know what the government is doing, and if the government does not detain or arrest them, they will not be able to complain that the government’s conduct caused them any harm.⁶¹ If they are

51. Justice Scalia does not like the *Katz* test, even though he uses it to reach the same result. He suggests a return to an original definition of “search” as looking over or through something or exploring or examining. *See id.* at 32–33, 32 n.1 (citing N. WEBSTER, AN AMERICAN DICTIONARY OF THE ENGLISH LANGUAGE 66 (6th ed. 1989) (1828)). He says that the Court “must take the long view, from the original meaning of the Fourth Amendment forward.” *Id.* at 40. Conceding “searches” in more cases, Justice Scalia would move the emphasis of the analysis to whether those governmental actions were “reasonable.” *See Amar, supra* note 7, at 760 n.4 (agreeing with Justice Scalia’s belief that reasonableness is the touchstone of the Fourteenth Amendment).

52. *Kyllo*, 533 U.S. at 40.

53. *Id.* at 47 (Stevens, J., dissenting).

54. *Id.* at 51.

55. *Id.* at 45.

56. *Id.*

57. *Id.*

58. *Id.* at 44.

59. *See id.* at 33–34 (declaring the difficulty of setting limits to physical surveillance as technology advances).

60. *See* Christopher Slobogin, *Technologically-Assisted Physical Surveillance: The American Bar Association’s Tentative Draft Standards*, 10 HARV. J. L. & TECH. 383, 401–02 (lamenting that current case law leaves many issues with physical surveillance unaddressed).

61. *See, e.g., infra* subpart III(C).

detained or arrested, the government may find it easy under prevailing notions to demonstrate to a court that the physical surveillance did not constitute a search.⁶² Although the Supreme Court has not directly ruled on physical surveillance, its decisions, including *Kyllo*, take for granted that this type of governmental action is not a search.⁶³

In *United States v. Knotts*,⁶⁴ for example, the Supreme Court held that the government's installation and tracking of a radio beeper in a chemical drum was not a search.⁶⁵ To reach this result, the Court said that the beeper did not provide anything the police could not obtain—with more effort—through visual surveillance in public places.⁶⁶ The government tracked the drum between the chloroform's purchase in Minneapolis, Minnesota, and the defendant's cabin near Shell Lake, Wisconsin.⁶⁷ Thus, the tracking was not inside the defendant's home. Writing for the Court, Justice Rehnquist emphasized that this case was not about twenty-four-hour surveillance. As he said, "[I]f such dragnet type law enforcement practices . . . should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable."⁶⁸ Twenty-seven years later, the Supreme Court has still not returned to the issue which Rehnquist left open in *Knotts*: pervasive, physical surveillance.

B. *The Lower Courts*

The United States Supreme Court has not devoted many pages to "expectations of privacy" since 9/11.⁶⁹ Even its opinions related to the Fourth Amendment have been on other topics.⁷⁰ The lower courts, left alone,

62. See *infra* subpart III(C).

63. See *infra* notes 63–66 and accompanying text; cf. *California v. Ciraolo*, 476 U.S. 207, 213 (1986) (recognizing as legal under the Fourth Amendment an officer's observations of a suspect who knowingly exposes her activity to the public).

64. 460 U.S. 276 (1983).

65. *Id.* at 285.

66. *Id.* at 282.

67. *Id.* at 278.

68. *Id.* at 284.

69. See *supra* notes 59–60 and accompanying text.

70. See *Arizona v. Gant*, 129 S. Ct. 1710, 1716 (2009) (citing *Katz* to support the existence of exceptions to the warrant requirement) (holding that the exception that allows a warrantless search incident to arrest in a car applies only to the area in which the arrestee might grab a weapon or destroy evidence); *Brigham City, Utah v. Stuart*, 547 U.S. 398, 403 (2006) (citing *Katz* to support exceptions to the warrant requirement) (holding that a police officer may enter a home without a warrant if he has an objectively reasonable basis to believe an occupant is seriously injured or faces imminent serious injury); *Georgia v. Randolph*, 547 U.S. 103, 110, 114 (2006) (using *Katz* in the majority to separate Fourth Amendment rights from property law; in dissent, citing Justice Harlan's *Katz* concurrence as the outside limit of the Court's inquiry into expectations of privacy) (holding that consent disputed by a physically present co-inhabitant is no exception to the warrant requirement); *United States v. Grubbs*, 547 U.S. 90, 95 (2006) (citing *Katz* as an example of anticipatory warrants in the context of electronic surveillance) (holding that anticipatory warrants do not violate Fourth Amendment rights and that the Fourth Amendment does not require an anticipatory warrant to list its triggering condition); *Illinois v. Caballes*, 543 U.S. 405, 416 n.6

continue to answer difficult questions of whether government conduct constitutes a search.⁷¹ My goal in surveying these decisions is to determine how faithful lower courts are in applying Harlan's two-part test and how useful those two parts are to their analysis. In the federal courts of appeals, there is a range of faithfulness to Harlan's two-pronged approach for determining whether government action rises to a search. Some courts apply Harlan by the book.⁷² Other courts apply some but not all of Harlan.⁷³ And still others ignore him, taking another approach.⁷⁴

1. *Application of Harlan*

a. Strict Adherence to Harlan's Test.—The federal courts of appeals that faithfully apply Harlan's test conduct a formal analysis of both prongs. The Seventh Circuit, for example, said the following in deciding whether police entry into the common area of a duplex was a search:

[Defendant] has not demonstrated a subjective expectation of privacy with respect to the common hallway. Nor has he shown that any subjectively held expectation of privacy that he might hold with respect to that hallway is one that society is prepared to recognize as reasonable Exposing the activities within the common hallway to the world is inconsistent with a subjective expectation of privacy

Even if [defendant] held a subjective expectation of privacy with respect to the common hallway, the facts of this case and our precedents reveal that such an expectation would not be "one that society is prepared to recognize as reasonable."⁷⁵

This is straight from Harlan.⁷⁶ Similarly, the Eleventh Circuit formally used both of Harlan's prongs. In *United States v. King*,⁷⁷ the defendant stored child pornography on a common network drive but took steps to secure access to his own computer.⁷⁸ The Court ruled that "[h]is experience

(2005) (citing *Katz* in dissent to demonstrate a manifestation of an expectation of privacy) (holding that a dog sniff around an automobile's exterior during a routine traffic stop does not require reasonable suspicion); *Groh v. Ramirez*, 540 U.S. 551, 561 (2004) (citing *Katz* for the necessity of magistrate-imposed restraint) (holding that a warrant that fails to describe the evidence sought is invalid and that a search pursuant to this warrant is unreasonable for lack of oversight by a magistrate).

71. *See infra* Part III.

72. *See infra* subsection III(B)(1)(a).

73. *See infra* subsection III(B)(1)(b).

74. *See infra* section III(B)(2).

75. *United States v. Villegas*, 495 F.3d 761, 767 (7th Cir. 2007) (quoting *United States v. Yang*, 478 F.3d 832, 835 (7th Cir. 2007)).

76. *See Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) ("[T]here is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'").

77. 509 F.3d 1338 (11th Cir. 2007).

78. *Id.* at 1339.

with computer security and the affirmative steps he took to install security settings demonstrate a subjective expectation of privacy in the files, so the question becomes ‘whether society is prepared to accept [King’s] subjective expectation of privacy as objectively reasonable.’”⁷⁹ Moving to the second prong, the court found that “[b]ecause his expectation of privacy was unreasonable King suffered no violation of his Fourth Amendment rights when his computer files were searched through the computer’s connection to the base network.”⁸⁰

The federal courts of appeals that faithfully and consistently adhere to Harlan are the Second,⁸¹ Seventh,⁸² Tenth,⁸³ Eleventh,⁸⁴ and the D.C.

79. *Id.* at 1341–42 (quoting *United States v. Hall*, 47 F.3d 1091, 1097 (11th Cir. 1995)).

80. *Id.* at 1342.

81. *See MacWade v. Kelly*, 460 F.3d 260, 272–73 (2d Cir. 2006) (holding that New York subway riders have a subjective expectation of privacy in the bags they carry into the subway, an expectation the Supreme Court has recognized as objectively reasonable); *United States v. Titemore*, 437 F.3d 251, 258 (2d Cir. 2006) (examining whether the defendant manifested a subjective expectation of privacy in part of a curtilage and whether society would recognize it as reasonable); *Palmieri v. Lynch*, 392 F.3d 73, 81 (2d Cir. 2004) (using the headings “subjective expectation of privacy” and “objectively reasonable expectation of privacy” for its analysis).

82. *See Michael C. v. Gresbach*, 526 F.3d 1008, 1015 (7th Cir. 2008) (“Private schools, by their very operation, exhibit a subjective expectation of privacy. . . . Moreover, an expectation of privacy is objectively reasonable where parents . . . expect that the parents’ express delegation of parental authority to school officials will be both acknowledged and respected by government actors.” (citations omitted)); *United States v. Figuero-Espana*, 511 F.3d 696, 704 (7th Cir. 2007) (“Without evidence suggesting that [he] was driving the truck with someone else’s permission, he cannot establish that he had a subjective expectation of privacy in the vehicle. Nor can he establish an objective expectation of privacy . . . [because he] failed to produce a valid driver’s license”); *United States v. Amaral-Estrada*, 509 F.3d 820, 827 (7th Cir. 2007) (reasoning that the defendant “failed to manifest any . . . actual or subjective expectation of privacy” in a vehicle he was borrowing and therefore did not exhibit any legitimate expectation of privacy); *Christensen v. County of Boone, Ill.*, 483 F.3d 454, 459–60 (7th Cir. 2007) (holding that there was no subjective or objectively reasonable expectation of privacy while driving on public streets or parking in a business parking lot); *United States v. Yang*, 478 F.3d 832, 836 (7th Cir. 2007) (“Because Yang had no subjective expectation of privacy in the notebooks, we need not reach the objectively reasonable injury.”); *United States v. Mendoza*, 438 F.3d 792, 795–96 (7th Cir. 2006) (analyzing the search of a garage through Harlan’s two-pronged test).

83. *See United States v. Worthon*, 520 F.3d 1173, 1182–83 (10th Cir. 2008) (“Mr. Romero unquestionably maintained no subjective expectation of privacy over the bags in the van. . . . [He also] made no showing that . . . would have allowed him to drive the car legitimately.” (quoting *United States v. Roper*, 918 F.2d 885, 887 (10th Cir. 1990))); *United States v. Barrows*, 481 F.3d 1246, 1248–49 (10th Cir. 2007) (holding that a personal computer Mr. Barrows brought to work from his home to use for common office functions may have established a subjective expectation of privacy, but not a reasonable expectation of privacy that society would recognize); *United States v. Hatfield*, 333 F.3d 1189, 1198 (10th Cir. 2003) (“Even though we can conclude that Hatfield had a subjective expectation of privacy in the space immediately behind his house, this is not an expectation of privacy that society regards as reasonable, at least with respect to visual observations made from an adjoining open field.”); *United States v. Rhiger*, 315 F.3d 1283, 1285–87 (10th Cir. 2003) (examining when a social guest establishes a subjective and legitimate expectation of privacy); *United States v. Higgins*, 282 F.3d 1261, 1272 (10th Cir. 2002) (“The facts that he had brought some personal property to the premises and that he had plans to reside there in the future may speak to his subjective expectation of privacy, but they fall short of establishing circumstances on which an objectively reasonable expectation of privacy could be based.”); *United States v. Angevine*, 281 F.3d 1130, 1134 n.1 (10th Cir. 2002) (“Because we conclude society is not prepared

Circuits.⁸⁵ The Ninth Circuit also applies Harlan's framework consistently⁸⁶ but sometimes drifts into the language of a "legitimate expectation" as shorthand for the two prongs.⁸⁷

Finally, while the First Circuit has sometimes used Harlan's test,⁸⁸ it does not always do so. In *United States v. Paradis*,⁸⁹ the court only used a reasonable expectation standard,⁹⁰ never referring to the two prongs. In *United States v. Dunning*,⁹¹ the court set up Harlan's framework when it stated that the "[defendant] contends that he had an expectation of privacy in a letter sent to a girlfriend with whom he had an intimate relationship and an understanding that the two would save their letters to each other, and that this expectation ought to be recognized as reasonable."⁹² However, the court dismissed the two-pronged approach and applied a "legitimate and reasonable

to recognize as reasonable an expectation of privacy in the seized University computer, we need not consider whether Professor Angevine himself had a subjective expectation of privacy.").

84. See *United States v. Segura-Baltazar*, 448 F.3d 1281, 1286–87 (11th Cir. 2006) (analyzing the subjective and objective expectations of privacy for garbage placed near the curb for the trash collector); *United States v. Miravalles*, 280 F.3d 1328, 1331–33 (11th Cir. 2002) (holding that there is neither a subjective nor objectively reasonable expectation to privacy in a large, high-rise apartment building, where the front door has an undependable lock).

85. See *United States v. Askew*, 529 F.3d 1119, 1127 (D.C. Cir. 2008) ("By zipping up his jacket, appellant unquestionably evidenced an intent to keep private whatever lay under it. The only question, then, is whether society is prepared to recognize such an expectation as reasonable."); *Stewart v. Evans*, 351 F.3d 1239, 1243–44 (D.C. Cir. 2003) (holding that even if defendant held a subjective expectation of privacy in documents transferred from her place of employment, it was not a reasonable one).

86. See *United States v. Forrester*, 512 F.3d 500, 509–11 (9th Cir. 2008) (using Harlan's framework to analyze the computer surveillance techniques that reveal the to/from addresses of e-mail messages, the IP addresses of Web sites visited, and the total amount of data transmitted to or from an account); *United States v. Diaz-Castaneda*, 494 F.3d 1146, 1151 (9th Cir. 2007) (holding that people have neither a subjective nor an objectively reasonable expectation of privacy in a license plate); *United States v. Heckenkamp*, 482 F.3d 1142, 1146 (9th Cir. 2007) ("The government does not dispute that [he] had a subjective expectation of privacy in his computer and his dormitory room, and there is no doubt that [his] subjective expectation . . . was legitimate and objectively reasonable.").

87. See *United States v. Davis*, 332 F.3d 1163, 1167–68 (9th Cir. 2003) ("[W]e do not conclude[] that Davis had less of a legitimate expectation of privacy in his gym bag than one would have in a suitcase [or] a purse [B]y placing his gym bag under the bed, Davis 'manifested an expectation that the contents would remain free from public examination.'" (citations omitted)).

88. See *United States v. Rheault*, 561 F.3d 55, 59 (1st Cir. 2009) ("We are satisfied that Rheault's decision to place the gun and drugs inside the washing machine on the third-floor landing sufficiently evidences an intent to hide them, and thus demonstrates a subjective expectation of privacy. . . . [W]e next turn to the much closer question of whether Rheault's subjective expectation was reasonable."); *United States v. Samboy*, 433 F.3d 154, 161 (1st Cir. 2005) ("We find that Samboy failed to argue his subjective privacy interest in the third-floor apartment in the court below. Moreover, Samboy has not pointed to any evidence to show that his interest in the apartment was one society would recognize as reasonable.").

89. 351 F.3d 21 (1st Cir. 2003).

90. See *id.* at 27, 32 (discussing only whether the defendant had a reasonable expectation of privacy and omitting any discussion of a two-pronged test).

91. 312 F.3d 528 (1st Cir. 2002).

92. *Id.* at 530–31.

expectation” standard, citing the Supreme Court’s decision in *Rakas v. Illinois*.⁹³ This is a sign that the First Circuit is not as faithful to Harlan as its other decisions suggest; the *Rakas* Court cited Justice Stewart’s majority opinion in *Katz*—not Harlan’s concurrence—as support for a test that determines “whether the person who claims the protection of the Amendment has a legitimate expectation of privacy in the invaded place.”⁹⁴ The *Dunning* opinion is an outlier, as later First Circuit decisions applied Harlan’s framework.⁹⁵ Yet even in a circuit that is generally faithful to Harlan, there is a sign of a return to a simpler framework.

b. Relaxed Adherence to Harlan’s Test.—There are other courts of appeals that cite Harlan’s framework but then proceed with a derivative standard. We might refer to this as relaxed adherence. The Sixth Circuit, for example, explained:

In analyzing whether a subjective expectation of privacy is objectively reasonable, this court considers a number of factors: (1) whether the defendant was legitimately on the premises; (2) his proprietary or possessory interest in the place to be searched or the item to be seized; (3) whether he had the right to exclude others from the place in question; and (4) whether he had taken normal precautions to maintain his privacy.⁹⁶

The first and second factors, of course, are a throwback to the pre-*Katz* framework on what is a search under the Fourth Amendment.⁹⁷ The Sixth Circuit, in another opinion, identified an additional factor: “whether [the defendant] has exhibited a subjective expectation that the area would remain free from governmental intrusion.”⁹⁸ The Fifth and Eighth Circuits also used these additional factors to decide subjective and objectively reasonable expectations of privacy.⁹⁹ While the Fifth, Sixth, and Eighth Circuits may be faithful to Harlan’s framework by accepting his labels and packaging, their lists of factors function more like Stewart’s totality-of-the-circumstances test.

93. *Id.* at 531 (citing *Rakas v. Illinois*, 439 U.S. 128, 143 (1978)).

94. *Rakas*, 439 U.S. at 143.

95. See *United States v. Rheault*, 561 F.3d 55, 59 (1st Cir. 2009) (using the two-part test for the expectation of privacy question); *United States v. Samboy*, 433 F.3d 154, 161 (1st Cir. 2005) (holding that there is no expectation of privacy because the defendant failed to argue a subjective privacy interest and because there is no evidence that the interest is one that society would recognize as reasonable).

96. *United States v. Dillard*, 438 F.3d 675, 682 (6th Cir. 2006).

97. See *United States v. Katz*, 389 U.S. 347, 352–53 (1967) (eschewing past cases that had used trespass standards and property interests in determining the applicability of the Fourth Amendment).

98. *United States v. Waller*, 426 F.3d 838, 844 (6th Cir. 2005).

99. See *United States v. Finley*, 477 F.3d 250, 258–59 (5th Cir. 2007) (using the factors to determine whether the defendant had a privacy interest in a company-issued cell phone); *United States v. Mendoza*, 281 F.3d 712, 715 (8th Cir. 2002) (applying the factors in deducing whether Mendoza had a legitimate expectation of privacy in a common area entryway in a duplex); *United States v. Runyan*, 275 F.3d 449, 457 (5th Cir. 2001) (using the factors to determine whether the defendant had a reasonable expectation of privacy in items found at his ranch).

Other opinions in the Fourth, Sixth, and Eighth Circuits cite the two-pronged approach but then gloss over the subjective expectation of privacy to focus only on the reasonable expectation prong. In a case about aerial surveillance, the Eighth Circuit “assume[d] without deciding that [the defendant] had a subjective expectation of privacy and focus[ed] on whether such an expectation could be objectively reasonable.”¹⁰⁰ The Fourth and Sixth Circuits have also acknowledged Harlan’s framework without coming back to it.¹⁰¹

The Fourth and Eighth Circuits also have outliers. In *United States v. Stevenson*,¹⁰² the Fourth Circuit discussed the two prongs in detail with specific facts from the record.¹⁰³ The Eighth Circuit, in analyzing whether a tape recording was a search, reasoned that “[the defendant] acknowledged, near the end of the conversation, that his statements were being recorded, and that this was ‘fine’ with him. Under these circumstances, [the defendant] could not reasonably expect that the conversation was private, and there was no search within the meaning of the Fourth Amendment.”¹⁰⁴ Nevertheless, both decisions are flanked by others that put their respective circuits within a camp of relaxed adherence to Harlan.

2. *Departure from Harlan.*—The Third Circuit departed from Harlan’s two-pronged framework to use the “legitimate expectation of privacy” standard from *Rakas*. In *United States v. Perez*,¹⁰⁵ the Third Circuit cited *Rakas* for the notion that the Fourth Amendment protects against searches where persons have “a legitimate expectation of privacy in the invaded place.”¹⁰⁶ It further explained:

Under this rule, persons in another’s apartment for a short time for the business purpose of packaging cocaine had no legitimate expectation

100. *United States v. Boyster*, 436 F.3d 986, 992 (8th Cir. 2006); *see also* *United States v. Brown*, 408 F.3d 1049, 1051 (8th Cir. 2005) (“There was no evidence Brown had a reasonable expectation of privacy in Lewis’s residence, because he was not present during the search, did not live at the residence, and did not have a key to the residence.”); *United States v. Hill*, 393 F.3d 839, 841 (8th Cir. 2005) (“These cases recognize that regardless of one’s subjective expectation of privacy in a public restroom, society’s recognition of that expectation of privacy is limited by the physical design of the restroom, [its] location . . . , and the probability that one will be asked to surrender use of the restroom to others.”).

101. *See* *United States v. Gray*, 491 F.3d 138, 145–46 (4th Cir. 2007) (analyzing whether the defendant was a social or business guest in Gray’s apartment and the appropriate level of privacy based on societal expectations); *United States v. Ellison*, 462 F.3d 557, 560–62 (6th Cir. 2006) (examining the reasonable expectations of a vehicle’s license plate); *United States v. Breza*, 308 F.3d 430, 433–35 (4th Cir. 2002) (determining the reasonable privacy expectations with regard to aerial surveillance of the curtilage).

102. 396 F.3d 538 (4th Cir. 2005).

103. *See id.* at 546–47 (analyzing whether the defendant, having shown an intention not to return to his apartment, had a reasonable expectation of privacy after his arrest).

104. *Sherbrooke v. City of Pelican Rapids*, 513 F.3d 809, 815 (8th Cir. 2008).

105. 280 F.3d 318 (3d Cir. 2002).

106. *Id.* at 337 (quoting *Minnesota v. Carter*, 525 U.S. 83, 88 (1998)).

of privacy in that apartment. Thus any search which may have occurred did not violate their Fourth Amendment rights. Although overnight guests who are legitimately in a third-party's apartment may have a reasonable expectation of privacy, Appellants do not qualify.¹⁰⁷

However, the Third Circuit has shown some fidelity to Harlan's framework by applying factors used by the Fifth, Sixth, and Eighth Circuits.¹⁰⁸ Even so, the Third Circuit's emphasis on places and privacy in other cases leaves *Perez* as an example of a departure from the two-pronged approach.¹⁰⁹ The Third Circuit thus welcomes Stewart over Harlan.

In the other circuits, Stewart's approach would obviate a mechanical application of Harlan's first prong, freeing the analysis to apply as many factors as are helpful to the specific facts of the case. Trespass is no longer an important factor, but the duration and the intensity of governmental action still matters to people protected by the Fourth Amendment. A return to Stewart would recognize all this in simpler terms.

C. Shortcomings of the Legal Framework

We have time before the next attack to reach a better equilibrium on physical surveillance. Related to the subway scenario that started this Article, I considered three types of surveillance: cameras, goggles, and detectors.¹¹⁰ Since the thwarted Christmas bombing plot in 2009¹¹¹ and President Obama's call to install more see-through scanners in American airports,¹¹² the public has been reminded that surveillance is not just an academic topic. Of the three forms of surveillance in our scenario, goggles would seem to present the most problems under the current Fourth Amendment framework.

107. *Id.* (citation omitted).

108. *See Warner v. McCunney*, 259 F. App'x 476, 477 (3d Cir. 2008) (using four factors that are relevant to showing a legitimate expectation of privacy: whether the party had a possessory interest, whether it could exclude others from the place, whether it took precautions to maintain privacy, and whether it had a key to the premises); *United States v. Hartwell*, 436 F.3d 174, 177 n.4 (3d Cir. 2006) (citing to *Kyllo* for the two-pronged approach but not analyzing the search because the government conceded the point).

109. *See Miller v. Hassinger*, 173 F. App'x 948, 952 (3d Cir. 2006) (citing *Minnesota v. Carter*, 525 U.S. 83, 88 (1998)) (providing that to demonstrate a constitutional privacy interest, an individual must establish a reasonable expectation of privacy in the place searched); *United States v. Schofield*, 80 F. App'x 798, 802 (3d Cir. 2003) (noting that the defendant must have a reasonable expectation of privacy in the automobile to have standing to challenge the search).

110. *See supra* notes 18–26 and accompanying text.

111. *See Mark Hosenball et al., The Radicalization of Umar Farouk Abdulmutallab*, NEWSWEEK, Jan. 11, 2010, at 37, 37 (discussing Abdulmutallab's personal background and the steps he took in his failed attempt to ignite an explosive device on a plane on Christmas Day 2009).

112. *See Associated Press, Body Scanners at More Airports: Passengers Can Choose Metal Detectors, Patdown Instead*, GRAND RAPIDS PRESS, Mar. 14, 2010, at J4 (noting that the Obama Administration set aside \$1 billion of the \$787 billion stimulus package for airport screening, \$25 million of which was for body scanners).

The cameras on the agents' helmets would be recording people in public places; plus, those recordings would not be broadcast on television or the Internet. When a citizen walks down the street, he accepts that other people may be watching him—in the same way that cameras may be recording him.¹¹³ So, even if the United States veered toward the British practice of CCTV, it would not present a constitutional problem under current law or under my proposed reappraisal of the Fourth Amendment.¹¹⁴ In reaching these conclusions, I assume that the cameras perform a general scan of the crowd without zooming in on a person unless there is a particularized suspicion.

Similarly, the radiation detectors are safe under current law. The detectors, to be sure, are not limited to surface readings of people's movements. Even so, in line with Justice Stevens, I doubt people expect privacy for the radiological emanations of their belongings.¹¹⁵ Such expectations would not be legitimate.¹¹⁶ An agent who detects radiation with the assistance of basic technology is not different for purposes of the law from an agent who detects the smell of alcohol or marijuana from a suspect on the street. Neither the detection nor the smelling involves a search.¹¹⁷

113. Cf. John Buntin, *Long Lens of the Law*, GOVERNING, May 2009, at 24, available at <http://www.governing.com/article/long-lens-law> (praising security cameras as “force multipliers” that would allow a single police officer at a monitor to perform the surveillance work of several officers in the field).

114. See *Kyllo v. United States*, 533 U.S. 27, 31–32 (2001) (explaining that although “‘at the very core’ of the Fourth Amendment ‘stands the right of a man to retreat into his own home and there be free from unreasonable government intrusion,’” this has never “‘require[d] law enforcement officers to shield their eyes when passing by a home on public thoroughfares’” (quoting *Silverman v. United States*, 365 U.S. 505, 511 (1961); *California v. Ciraolo*, 476 U.S. 207, 213 (1986))); *Dow Chem. Co. v. United States*, 476 U.S. 227, 238–39 (1986) (holding that aerial photography of a vast industrial complex did not constitute a search for Fourth Amendment purposes because there was no reasonable expectation of privacy); *Katz v. United States*, 389 U.S. 347, 361 (1967) (noting that “objects, activities, or statements that [a person] exposes to the ‘plain view’ of outsiders are not ‘protected’ because no intention to keep them to himself has been exhibited”).

115. See *Kyllo*, 533 U.S. at 43–44 (2001) (Stevens, J., dissenting) (“Heat waves . . . enter the public domain A subjective expectation that they would remain private is not only implausible but also surely not ‘one that society is prepared to recognize as “reasonable.”’” (quoting *Katz*, 389 U.S. at 361 (Harlan, J., concurring))).

116. See, e.g., *California v. Greenwood*, 486 U.S. 35, 39–40 (1987) (holding that even if petitioners may have subjectively expected the contents to remain private, there is no legitimate expectation of privacy in trash left for collection in an area accessible to the public because society has not recognized an objectively reasonable expectation of privacy in such items); *id.* at 41 (“[A]s we have held, the police cannot reasonably be expected to avert their eyes from evidence of criminal activity that could have been observed by any member of the public.”); *United States v. Jacobsen*, 466 U.S. 109, 122 (1984) (“The concept of an interest in privacy that society is prepared to recognize as reasonable is, by its very nature, critically different from the mere expectation, however well justified, that certain facts will not come to the attention of the authorities.”); *supra* text accompanying note 39.

117. Cf. *United States v. Place*, 462 U.S. 696, 707 (1983) (holding that the use of a drug dog to detect drugs does not constitute a search under Fourth Amendment case law because the procedure

People do not have a legitimate expectation in the emanations of things they carry with them or in the smells, sounds, or sights they emit from their bodies. The governmental action to detect these things is not usually intense or longstanding.¹¹⁸

The goggles, unlike the cameras and the radiation detectors, see through a person's clothes. People, guilty or innocent, suspicious or inconspicuous, will be naked to the agents' eyes. The agents may see who has a replaced hip, a steel implant in the skull, or a pacemaker. Many people want to keep these facts private. If the devices detect plastics in addition to metals, the privacy concerns are more obvious. Some women do not want the world to know whether the contours to their bodies have been shaped, not by nature, but by a surgeon's scalpel.

My goal, to repeat, is to show *Katz's* limitations in protecting American privacy. Perpetual surveillance occurs with some suspects today; its relevance does not depend on another attack. The scenario about a subway attack serves as a reminder that physical surveillance can easily become very intrusive. As a result, a basic totality-of-the-circumstances test, rather than Justice Harlan's two-part test, is more useful in reaching the common-sense conclusion that at some point, 24/7 surveillance becomes intrusive enough to constitute a search. A search by the government then requires probable cause, reasonable suspicion, or, if individual suspicion is not there, some special need.¹¹⁹ Since the courts have recognized that there is a point at which a canine sniff can become intrusive enough to be a search,¹²⁰ they should be more forthright in recognizing that physical surveillance can switch categories just as easily. To me, Stewart's test seems more flexible than Harlan's for factoring the duration and the intensity of governmental action into the constitutional equation.

is limited "both in the manner in which the information is obtained and in the content of the information revealed by the procedure").

118. See *infra* subpart IV(C).

119. See U.S. CONST. amend. IV ("[N]o Warrants shall issue, but upon probable cause, supported by Oath or affirmation . . ."); *Illinois v. Lidster*, 540 U.S. 419, 424 (2004) (upholding the constitutionality of "information stops" and reiterating that searches absent particularized individual suspicion may be constitutional under the Fourth Amendment if special law enforcement purposes—other than general law enforcement—exist); *United States v. Arvizu*, 534 U.S. 266, 273 (2002) (reaffirming that, in some instances, a standard less than probable cause—"reasonable suspicion"—can support the reasonableness of a search in accordance with the Fourth Amendment).

120. See *United States v. Kelly*, 302 F.3d 291, 293 n.1 (5th Cir. 2002) (holding that up-close canine sniffing offends reasonable expectations of privacy and is therefore a search under the Fourth Amendment but that such searches, if routine, are permissible under the border-search exception to the warrant requirement); *B.C. v. Plumas Unified Sch. Dist.*, 192 F.3d 1260, 1266 (9th Cir. 1999) (holding that canine sniffs of high school students are Fourth Amendment searches); *United States v. Thomas*, 757 F.2d 1359, 1367 (2d Cir. 1985) (holding that a canine sniff outside an apartment door for the purposes of detecting drugs is a Fourth Amendment search). *But see United States v. Reed*, 141 F.3d 644, 649 (6th Cir. 1998) (holding that a canine sniff is not a search within the meaning of the Fourth Amendment).

Justice Stewart's totality-of-the-circumstances test does not eliminate ambiguity. No test can. Those who lean toward bright lines might actually prefer the emphasis on trespass that characterized Fourth Amendment jurisprudence before *Katz*.¹²¹ They may challenge both Justice Harlan and Justice Stewart. An advantage of the trespass test is that it avoids murky inquiries about expectations of privacy. The trespass test does not purport to determine whether sight, sound, or smell is more intrusive. Instead, trespass is about simple touch.¹²² As long as government agents do not touch suspects, do not touch their things, and do not stand on their property, the agents should be fine under the Fourth Amendment. Even under the law before *Katz*, constant surveillance was acceptable as long as it followed these rules. The time has come for change.

IV. Breakdown of the Framework

I am certainly not the first to criticize the Court's test for expectations of privacy.¹²³ But I am probably the most explicit, since 9/11, to suggest Justice Stewart's test as the replacement.

121. See *Kyllo v. United States*, 533 U.S. 27, 31 (2001) ("The permissibility of ordinary visual surveillance of a home used to be clear because, well into the 20th century, our Fourth Amendment jurisprudence was tied to common-law trespass." (citing *Goldman v. United States*, 316 U.S. 129, 134–36 (1942); *Olmstead v. United States*, 277 U.S. 438, 464–66 (1928))); cf. *Silverman v. United States*, 365 U.S. 505, 510–12 (1961) (relying on whether an "actual intrusion into a constitutionally protected area" had occurred rather than whether there had been a technical trespass in determining whether a Fourth Amendment search had occurred).

122. See *Olmstead*, 277 U.S. at 465–66 (holding that the Fourth Amendment applies only to physical searches and not to searches "by hearing or sight").

123. See, e.g., Amsterdam, *supra* note 9, at 385 (arguing that *Katz* "offers neither a comprehensive test of fourth amendment coverage nor any positive principles by which questions of coverage can be resolved"); Laurence A. Benner, *Diminishing Expectations of Privacy in the Rehnquist Court*, 22 J. MARSHALL L. REV. 825, 852 (1989) ("[T]he outcome of the *Katz* mode of analysis has increasingly resulted in the total loss of Fourth Amendment protection."); Marc Jonathan Blitz, *Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World That Trades Image and Identity*, 82 TEXAS L. REV. 1349, 1363 (2004) (arguing that Fourth Amendment jurisprudence "needs rethinking if constitutional privacy protections are to work well in twenty-first century conditions"); Morgan Cloud, *The Fourth Amendment During the Lochner Era: Privacy, Property, and Liberty in Constitutional Theory*, 48 STAN. L. REV. 555, 616–17 (1996) ("[O]ver the past thirty years the *Katz* approach has degenerated into a standardless 'expectations' analysis that has failed to protect either privacy or property interests."); Morgan Cloud, *Rube Goldberg Meets the Constitution: The Supreme Court, Technology and the Fourth Amendment*, 72 MISS. L.J. 5, 28–29 (2002) ("After a third of a century, it is fair to conclude that *Katz* is a failure . . ."); 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, 724 (1988) (arguing that since *Katz*, "the Supreme Court has determined that individual expectations of government surveillance, even when guarded against, appears wholly irrelevant"); Roberto Iraola, *New Detection Technologies and the Fourth Amendment*, 47 S.D. L. REV. 8, 8–9 (2002) (arguing that the Court has struggled to keep up with technology and that "[i]n the last thirty years, a number of investigative techniques—all found to fall outside the ambit of Fourth Amendment protection—have enabled the government to obtain details about our lives"); John M. Junker, *The Structure of the Fourth Amendment: The Scope of the Protection*, 79 J. CRIM. L. & CRIMINOLOGY 1105, 1183 (1989) ("The doctrinal record during the twenty years since *Katz*

A. *Academic Opinions and Problems*

Many scholars criticize the *Katz* framework for not doing enough to protect people against government snooping. Of those that criticize, however, very few wade into the differences between Stewart and Harlan. Their proposals for replacements can be broken into several groups—although I am mindful of the irony of doing so in an Article that says not to lose sight of the totality of circumstances.

A large group pushes for a return to a pre-*Katz* understanding of the Fourth Amendment, similar to the ruling in *Olmstead v. United States*.¹²⁴ This would tie the definition of a search to the concepts of property.¹²⁵ They

reveals a Court hostile to privacy and, of greater concern, willing to ignore or subvert the constraints of language and structure in its quest for the favored result.”); Lewis R. Katz, *In Search of a Fourth Amendment for the Twenty-First Century*, 65 IND. L.J. 549, 554 (1990) (declaring that “in the two decades since *Katz* was decided, the Court has applied the standard to reduce rather than enhance fourth amendment protections . . . allow[ing] the government access to many intimate details about our lives without having to establish the reasonableness of its behavior”); Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 826–27 (2004) (“Indeed, scholars consistently denounce the Court’s opinions interpreting *Katz* as ‘dead wrong,’ ‘off the mark,’ ‘misguided,’ and ‘inconsistent with the spirit of the fourth amendment.’” (citation omitted)); Tracy Maclin, Katz, Kyllo, and Technology: *Virtual Fourth Amendment Protection in the Twenty-First Century*, 72 MISS. L.J. 51, 51 (2002) (arguing that “the privacy and security protected by the Fourth Amendment should not depend on innovations in technology”); Christopher Slobogin, *Peeping Techno-Toms and the Fourth Amendment: Seeing Through Kyllo’s Rules Governing Technological Surveillance*, 86 MINN. L. REV. 1393, 1411 (2002) (arguing that *Katz* and its progeny do not sufficiently protect privacy since “[m]embers of our society should be constitutionally entitled to expect that government will refrain from any spying on the home—technological or otherwise—unless it can demonstrate good cause for doing so” (emphasis omitted)); William J. Stuntz, *Privacy’s Problem and the Law of Criminal Procedure*, 93 MICH. L. REV. 1016, 1048 (1995) (arguing that “[i]f we could start over, perhaps privacy would not receive constitutional protection anywhere”); George C. Thomas III, *Time Travel, Hovercrafts, and the Framers: James Madison Sees the Future and Rewrites the Fourth Amendment*, 80 NOTRE DAME L. REV. 1451, 1500 (2005) (“The ‘expectation of privacy’ notion is flawed to the core.”); James J. Tomkovicz, *Technology and the Threshold of the Fourth Amendment: A Tale of Two Futures*, 72 MISS. L.J. 317, 438 (2002) (asserting that *Kyllo* insufficiently protects privacy since “[o]fficial exploitation of a scientific or technological device should be considered a Fourth Amendment search”); Daniel B. Yeager, *Search, Seizure and the Positive Law: Expectations of Privacy Outside the Fourth Amendment*, 84 J. CRIM. L. & CRIMINOLOGY 249, 251 (1993) (“*Katz* has been a dismal failure . . .”).

124. 277 U.S. 438 (1928).

125. See Cloud, *The Fourth Amendment During the Lochner Era: Privacy, Property and Liberty in Constitutional Theory*, *supra* note 123, at 628 (arguing that the Fourth Amendment’s “ultimate purposes, rooted in the history of the Amendment, were to protect individual liberty, privacy, and property, and to preserve the capacity to enjoy all three in the quiet of one’s home or place of business”); Cloud, *Rube Goldberg Meets the Constitution: The Supreme Court, Technology and the Fourth Amendment*, *supra* note 123, at 47–50 (arguing that the jurisprudence should “emphasize the notion that the technological equivalent of a physical trespass can trigger a Fourth Amendment violation” as well as “extend this notion to settings outside of the interior of the home. At the very least, this should include other property that has traditionally received Fourth Amendment protection, including the home’s curtilage, closed containers like luggage, and the interior private commercial buildings,” and that “[t]his amalgam of property law, trespass theory, and technology could readily be extended to other settings”); see also Blitz, *supra* note 123, at 1364. Blitz argues that, as opposed to *Katz*’s famous pronouncement,

say when the government intrudes on a citizen's property, be it with the aid of technology or by physical entry, it should be a search. Professor Cloud, for example, contends that the "linkage between property, privacy, and liberty was more effective than is [the *Katz* rule] at implementing the Amendment's purposes and was more consistent with its text and history."¹²⁶ These critics say *Katz* changed very little of the analysis, since judges simply fall back on the time-tested rules of property law.¹²⁷

A second group pushes for a return to a more original interpretation of the Fourth Amendment,¹²⁸ comparable to what Scalia suggests in *Kyllo*.¹²⁹ For them, *Katz* has diluted the Fourth Amendment to allow police powers beyond the founders' vision. As Professor Davies argues, the "authentic history shows that framing-era doctrine provided a much stronger notion of a 'right to be secure' in person and house than does modern doctrine."¹³⁰ The originalists would more directly align the definition of a search with persons, houses, papers, and effects.¹³¹

[C]ourts 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.

Id. (emphasis omitted); see also Slobogin, *supra* note 123, at 1411 (arguing that our society should be constitutionally protected from "any spying on the home—technology or otherwise—unless it can demonstrate good cause for doing so" (emphasis omitted)).

126. Cloud, *The Fourth Amendment During the Lochner Era: Privacy, Property and Liberty in Constitutional Theory*, *supra* note 123, at 563.

127. See, e.g., Orin S. Kerr, *Technology, Privacy, and the Courts: A Reply to Colb and Swire*, 102 MICH. L. REV. 933, 934 (2004) ("Even when purporting to protect privacy, judges have proven reluctant to deviate from rules based on principles of property law.").

128. See Benner, *supra* note 123, at 830 ("[F]or the Framers, the heart of the Fourth Amendment lay in the requirement that *individualized* justification be established under oath, as a necessary predicate to governmental intrusion."); Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 724 (1999) ("The Framers aimed the Fourth Amendment precisely at banning Congress from authorizing use of general warrants; they did not mean to create any broad reasonableness standard for assessing warrantless searches and arrests."); Thomas, *supra* note 123, at 1458 (explaining his method of inquiry as understanding "the common law relevant to search and seizure and the political context in which the Fourth Amendment was proposed and debated" and with this in mind proposing "a series of modifications based on what I think the Framers would have said if they could have seen particular modern police methods.").

129. See *Kyllo v. United States*, 533 U.S. 27, 35 (2001) (arguing that defining the term "search" to include obtaining information about the interior of the home that the government could not otherwise get without physical intrusion would provide the level of protection against government that existed at the time of the adoption of the Fourth Amendment); *supra* notes 41–54 and accompanying text.

130. Davies, *supra* note 128, at 749.

131. See Thomas, *supra* note 123, at 1459 ("[T]he Court's attempt to expand the coverage of the Fourth Amendment by restating it as protecting privacy is a failure. We need to return to the plain meaning of 'persons, houses, papers, and effects' as those items would be understood by the Framers in the context of modern life.").

A third group shifts away from the Search and Seizure Clause to highlight the Warrant Clause¹³² or the role that Congress should play.¹³³ One scholar proposes a bright-line rule: “[A]ll government use of sophisticated visual equipment . . . should be subject to the warrant requirement.”¹³⁴ Others say Congress is better suited than the Courts to address privacy in the context of rapid technological developments. Thus, it is up to the Legislature to develop “more nuanced, balanced, and accurate privacy rules when technology is in flux.”¹³⁵

Finally, similar to my position, a few scholars lend some support to Justice Stewart’s majority opinion, while criticizing *Katz*’s progeny.¹³⁶ For them, *Katz* is salvageable. According to Professor Swire, “[c]ourts could engage in a more substantive review of expectations of privacy in specific factual settings, and find that more categories of government action violate that test.”¹³⁷ For Swire and others, the solution to search problems depends on a threshold question. Professor Benner suggests asking “whether Fourth Amendment protection existed as a threshold matter, and then by

132. See, e.g., Amsterdam, *supra* note 9, at 417 (“A paramount purpose of the fourth amendment is to prohibit arbitrary searches and seizures as well as unjustified searches and seizures. The warrant requirement was the framers’ chosen instrument to achieve both purposes, and it should continue to be applied to those ends. . . .”); Gutterman, *supra* note 123, at 732 (“We must bring technology under the umbrella of the procedural protections of the warrant clause.”); David E. Steinberg, *Making Sense of Sense-Enhanced Searches*, 74 MINN. L. REV. 563, 629 (1990) (asserting that “[n]owhere is an appropriate application of the warrant clause more essential to protect the security promised by the fourth amendment” than for sense-enhancing technologies).

133. See Amsterdam, *supra* note 9, at 380 (arguing that effective control over police practices depends upon, among other things, the creation of new regulatory devices subject to court oversight); Raymond Shih Ray Ku, *The Founders’ Privacy: The Fourth Amendment and the Power of Technological Surveillance*, 86 MINN. L. REV. 1325, 1375–76 (2002) (arguing that the Fourth Amendment should be interpreted to require legislative approval of any governmental use of new technologies to better protect privacy against these new innovations).

134. Gutterman, *supra* note 123, at 733.

135. Kerr, *supra* note 123, at 807–08. “Legislatures do not offer a panacea, but they do offer significant institutional advantages over courts.” *Id.* at 807.

136. See Gutterman, *supra* note 123, at 666 (“The damage had been done in his *Katz* concurrence. By basing *Katz* on a subjective expectation analysis and thereby a risk-assumption theory, Justice Harlan subjected each and every member of society to unimagined risks.”); Junker, *supra* note 123, at 1178 (“*Katz*’ weakness, however, is also its strength. It bends in both directions.”); Katz, *supra* note 123, at 560–63 (arguing that *Katz* “provided a framework for ensuring freedom by protecting personal security”); Scott E. Sundby, “*Everyman*’s Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?”, 94 COLUM. L. REV. 1751, 1755–56 (1994) (arguing that *Katz* could be the framework for the future of trust in the government); Peter P. Swire, *Katz is Dead. Long Live Katz*, 102 MICH. L. REV. 904, 905 (2004) (arguing that with the development of new technology, *Katz* may be “dead for [its] core facts,” but that Fourth Amendment doctrine should continue to play a role in governing high-tech searches); James J. Tomkovicz, *Beyond Secrecy for Secrecy’s Sake: Toward an Expanded Vision of the Fourth Amendment Privacy Province*, 36 HASTINGS L.J. 645, 737 (1985) (proposing an “instrumental approach to resolving fourth amendment threshold questions [that] will further [the] realization of the full potential of the *Katz* revolution”); Yeager, *supra* note 123, at 308 (arguing that though the test is flawed, “[w]hen the government is behaving lawfully, *Katz* acts as a backstop, as a second look at whether the positive law fairly reflects a given defendant’s expectations”).

137. Swire, *supra* note 136, at 923.

determining whether that protection had, nevertheless, been waived because it was reasonably foreseeable that the details actually observed by the police would have also been observed by members of the public.”¹³⁸ A search has occurred if this threshold test is answered in the positive.¹³⁹

B. *Common-Sense Answers*

Justice Harlan’s two-part test cuts out the common sense necessary to decide whether governmental action is a search. Lost between two layers of analysis are facts about the depth and duration of the intrusion. The Fourth Amendment is as much about places as it is people. When we put ourselves into public settings—a train station, the airport, a subway car, or the street—we know other people are observing us, but our expectation is for these observations to be brief and fleeting. Don’t stare at me and I won’t stare at you. We blend into the crowd. But if someone looks at us for too long, we become self-conscious. Our anonymity has disappeared, and the exchange with the observer might become violent, romantic, or something in between. The tipping point from anonymity to being in the imaginary crosshairs is not precise. It could take five seconds or ten seconds, but we know when our space has been violated. These are obvious points, but the jurisprudence of searches tends to ignore them. Today the prevalence of CCTV in the private sector, rather than decrease a citizen’s constitutional protections, should mean that the government’s addition of visual surveillance more readily tips the balance toward a search under the Fourth Amendment.

Moreover, despite all the talk about expectations of privacy, it is not clear whether Justice Harlan had in mind a person’s expectations about all possible intrusions (public and private) or just public intrusions. Depending on the facts, a person may have a different assessment of whether a cop or a private citizen is lurking about, and society’s decision about what is reasonable may also be affected.

In practice, the cases do not often turn on the first part of the Harlan test. Many cases in state and federal courts are decided without reported opinions.¹⁴⁰ The defendant who files a motion to suppress will allege that he expected to be free of the government conduct. The government can try to show facts that rebut the defendant’s allegation or, conceding the first part of Harlan’s test, it can move on to the second part. Further, Harlan’s test has other problems. A pure application of Harlan’s test would allow the government to lessen and perhaps eliminate expectations by a ratcheting of more

138. Benner, *supra* note 123, at 871–72.

139. *See id.* at 872 n.214 (“By liberally construing the language of the Amendment to effect its purpose in protecting privacy as mandated by *Boyd v. United States*, 116 U.S. 616, 635 (1886), much of the need for a Katzian analysis would disappear.”).

140. *E.g.*, *United States v. Davis*, No. 09-30047, 2010 WL 610646 (C.D. Ill. Feb. 11, 2010); *Young v. Commonwealth*, No. 2007-CA-002049-MR, 2010 WL 323120 (Ky. Ct. App. Jan. 29, 2010); *State v. Hoskinson*, No. 2 CA-CR 2008-0408, 2009 WL 3068990 (Ariz. Ct. App. Sept. 25, 2009).

intrusive activity. Justice Harlan himself eventually recognized this problem. In dissent in *United States v. White*, he noted that the purpose of the Fourth Amendment is “to form and project, as well as mirror and reflect.”¹⁴¹ Subjectivity was balanced by some court-imposed objectivity.

More commonly in Fourth Amendment cases, the government concedes that the defendant had a subjective expectation of privacy and then moves on to contest whether the second part of the test has been met.¹⁴² These concessions collapse the test into one line of inquiry on whether the expectations are reasonable. Thus, the second prong becomes a means for applying Stewart’s test, whether or not the parties and the judges acknowledge it. Although Justice Stewart and Justice Harlan both agreed that the Fourth Amendment “protects people, not places,”¹⁴³ the Supreme Court and the lower courts have considered the location of the government activity as a factor in determining “reasonable” expectations.¹⁴⁴ Justice Scalia’s opinion in *Kyllo*, as one example, cannot be fully appreciated without remembering that the thermal imaging was directed at a home, arguably the most protected place.¹⁴⁵

Yet both *Olmstead* and Harlan’s *Katz* concurrence are out of date for the modern world. As seen in the debate between Justice Scalia and Justice Stevens in *Kyllo*, the distinctions between touch, sight, sound, and smell can break down.¹⁴⁶ Courts continue to guess at our expectations of privacy. Often people are too private to speak about their privacy. By taking you to the toilet, I discuss important things that squeamish judges and other people may avoid in their opinions and their conversations.

C. Harlan’s Test Exposed

Imagine you have entered a public bathroom at the airport in Minneapolis–Saint Paul. You pick the far stall because it is a bit larger than the others and because the stall next to it is empty. You clean the toilet lid before you sit down. You grab a piece of leftover newspaper from the floor, pull your pants down, and sit down to relieve yourself. Later you find out an

141. 401 U.S. 745, 786 (1971) (Harlan, J., dissenting).

142. See, e.g., *United States v. Heckenkamp*, 482 F.3d 1142, 1146 (9th Cir. 2007) (noting that the Government did not dispute that the defendant had a subjective expectation of privacy, then holding that his expectation was reasonable); *United States v. Goldsmith*, 432 F. Supp. 2d 161, 169 (D. Mass. 2006) (noting that even though the reasonableness of the defendant’s expectation of privacy was at issue, the Government did not dispute his subjective expectation of privacy).

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

144. See *supra* subpart III(B); see also, e.g., *Kyllo v. United States*, 533 U.S. 27, 37 (2001) (noting that in the home “all details are intimate details”); *United States v. King*, 509 F.3d 1338, 1342 (11th Cir. 2007) (concluding that there is no reasonable expectation for privacy from a government search conducted through a computer connection to a common network drive); *United States v. Villegas*, 495 F.3d 761, 767 (7th Cir. 2007) (holding that there is no reasonable expectation for privacy in a common hallway of a duplex).

145. *Kyllo*, 533 U.S. at 29.

146. See *supra* text accompanying notes 41–58.

airport policeman was “monitoring” you in one of three ways.¹⁴⁷ First, a deaf agent with no sense of smell could have been above you, wedged in the ceiling. He peered down at you through a small hole. He only saw you in the middle of your business, not watching your preparations or your use of toilet paper after you flushed. He did not see your genitalia, only the sight of you reading with your pants down. Second, a blind and deaf agent could have been standing on the toilet seat in the stall next to you. He only smelled what you were doing. Third, a blind agent with no sense of smell could have been standing on the next toilet seat. He only heard what you were doing. Luckily for you, you get to pick which possibility is true.

Does it make sense to talk about different expectations of privacy for these three scenarios? Can we predict what possibility you and others will find the least invasive? The most? Have we in society really determined which expectations of privacy in the toilet stall we find reasonable? Have empirical studies gone that far? And, if so, are they reliable?

The *Olmstead* test would find these intrusions not to be a search.¹⁴⁸ You were in a public place, and the agent did not trespass on your constitutionally protected space. Both the Stewart test and the Harlan test would struggle to determine whether these intrusions were searches—assuming the agent gathered information of your illegal activity from the intrusion, you were arrested, and you contested the agent’s activity in a motion to suppress. The Harlan test, however, pretends to be more objective than it is. This Article, choosing Stewart over Harlan, strives to end those pretensions once and for all. Stewart’s totality-of-the-circumstances test makes more sense and is a

147. The monitoring of public bathrooms is not always hypothetical. Courts have held that whether bathroom surveillance is a search can depend on the location of the officer and the design of the stall. See *Kroehler v. Scott*, 391 F. Supp. 1114, 1118 n.4 (E.D. Pa. 1975) (finding that the expectation of privacy is controlled by the nature of the activity rather than the physical characteristics of the stall, or the even length of time in the bathroom); *Kirsch v. State*, 271 A.2d 770, 772 (Md. Ct. Spec. App. 1970) (holding that an officer unlocking and opening a bathroom door at the clerk’s request after three men had occupied it for thirty minutes did not constitute a search). Compare *Brown v. State*, 238 A.2d 147, 150 (Md. Ct. Spec. App. 1968) (holding that an officer sticking his head over a stall partition performed a search), and *State v. Bryant*, 177 N.W.2d 800, 804 (Minn. 1970) (holding that an officer surveying a stall through an overhead vent performed a search because the stall was completely secluded from outside view and the doors and stall assured the occupants of their privacy), with *Moore v. State*, 355 So. 2d 1219, 1221 (Fla. Dist. Ct. App. 1978) (holding that a police officer looking through a one-half inch crack in the bathroom stall door is not a search), and *Buchanan v. State*, 471 S.W.2d 401, 404 (Tex. Crim. App. 1971) (holding that police surveillance from a concealed position above a bathroom stall with no door was not a search because defendant had no reasonable expectation of privacy). Notoriously, bathroom surveillance resulted in the arrest of U.S. Senator Larry Craig in the men’s bathroom at Minneapolis–St. Paul International Airport on suspicion of lewd conduct in June 2007. *Senator, Arrested at Airport, Pleads Guilty*, N.Y. TIMES, Aug. 28, 2007, at A19. Police were cracking down after several complaints of sexual activity in the airport’s main men’s room. An officer stationed in a stall arrested Sen. Craig after he made signals that indicated he “[wished] to engage in lewd conduct.” Report from Sgt. Dave Karsnia, Minneapolis Airport Police Dept. (June 26, 2007), available at http://media.washingtonpost.com/wp-srv/politics/ssi/craig_police_report_082807.pdf.

148. See *supra* notes 124–27 and accompanying text.

more realistic summary of how courts and commentators struggle to balance individual and governmental interests.

V. Conclusion

You may not worry about the prospect of an extensive Government Toilet Surveillance Program. But you should worry about government intrusions that will come after the next attack. We are all reasonable in expecting a rational framework for determining whether a government surveillance program that includes cameras, goggles, and radiation detectors will constitute a search at some point. Justice Stewart's totality-of-the-circumstances test is better than Justice Harlan's two-part test in distinguishing brief periods of physical surveillance from constant surveillance that lasts days, weeks, months, or years. And Justice Stewart's test is much better for analyzing situations when various methods of surveillance are all combined.