Western New England University School of Law

Western New England University School of Law Legal Studies Research Paper Series

No. 13-13

THE FOURTH AMENDMENT AND SURVEILLANCE IN A DIGITAL WORLD

Arthur Leavens

The Fourth Amendment and Surveillance in a Digital World

© Arthur Leavens†

Introduction

Like it or not, technology has profoundly changed the way we relate to one another and to our government. If electronic technology once played a supportive role in our lives, a take-it-or-leave-it tool of convenience, that is no longer so. In the digital age, technology is inescapably woven into the fabric of our lives, bringing with it a vastly enhanced capability of the government to surveill the citizenry. Not only does the government have increasingly powerful surveillance tools, but the citizens themselves – wittingly or not – in large measure enable that surveillance by using technology that exposes a wide swath of information that most would regard as quintessentially private. Any doubt in this regard was dispelled by the summer 2013 disclosures concerning the on-going surveillance by the National Security Agency. We learned that the government has the capacity to collect and instantly analyze huge amounts of data – e.g., phone records, cell-phone GPS data, credit-card transactions, E-Z pass usage – to identify persons wherever they may be and to track and record their activities and precise locations (in some instances right down to the specific floor of a building), all without ever seeing or listening to them.[1] That may be a comfort – we are told of terrorist plots thus foiled, lives thus saved;[2] it is surely a concern. But whether we are comforted, concerned, or both, these revelations underscore the need for clear normative boundaries for such surveillance.

Of course, state and federal governments can, and to some extent do, police themselves through statutes[3] and regulations.[4] However, as a federal constitutional matter, the Fourth

---

† Professor of Law, Western New England University School of Law. I would like to thank my colleagues Giovanna Shay, Bruce Miller, Julie Steiner, Sudha Setty, Matthew Charity, René Reich-Graefe and Barbara Noah for their encouragement and thoughtful comments on earlier drafts of this article and Dean Art Gaudio for providing support and assistance for this project. I would also like to thank the Ronald H. Brown Center for Civil Rights and Economic Development and the Journal for Civil Rights and Economic Development for inviting me to participate in its symposium, *Criminal Justice in the 21st Century: The Challenge to Protect Individual Freedoms, Civil Rights and Our Safety*.

[1] *See* James Risen & Eric Lichtblau, *How the U.S. Uses Technology to Mine More Data More Quickly*, N.Y. Times, June 9, 2013, at 1, 11.

[2] *See* Eric Schmitt, David E. Sanger & Charlie Savage, *Mining of Data is Called Crucial to Fight Terror*, N.Y. Times, June 8, 2013, at A1, A11.

[3] For example, 45 years ago, as part of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197 (codified as amended in scattered sections of 5 U.S.C., 18 U.S.C. and 42 U.S.C.), Congress enacted comprehensive statutory regulation of wiretapping and electronic eavesdropping in what has come to be known as Title III, subsequently upgraded in the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified 18 U.S.C. §§1367, 2232, 2510 -2521, 2701-2710, 3121-3126). States, too, have enacted statutory limits on police investigatory practices. *E.g.*, Mass. G.L. c. 276, § 1 (2013) (limiting evidentiary searches incident to arrest to "fruits, instrumentalities, contraband and other evidence of the crime for which the arrest has been made").

Amendment provides the sole protection, one crafted over 200 years ago in response to the concerns of a very different world. On its face, the amendment strikes the balance between governmental surveillance and our right to be free from it in a concise, straightforward way, protecting us in our persons, houses, papers and effects against unreasonable searches and seizures.[5] The critical question is, how does this ancient construct work in the face of burgeoning, constantly evolving technology?

Fourth Amendment protection, of course, has two components – coverage and content. The two are obviously related, but the threshold issue is coverage, without which there is no protection. On its face, Fourth Amendment coverage is limited to "searches and seizures," and so, for a particular mode of surveillance to be subject to the amendment's reasonableness requirement, it must be a "search."[6] The Supreme Court first addressed the question of whether electronic surveillance constitutes a Fourth Amendment search in *Olmstead v. United States,*[7] the Court holding that a wiretap of a home telephone was not a search because there was no physical intrusion into the home. This property-based approach to Fourth Amendment coverage continued for some 40 years[8] until the landmark decision in *Katz v. United States*,[9] in which the Court changed course, announcing that "the Fourth Amendment protects people, not places."[10] In his concurrence, Justice Harlan reduced that broad statement of the amendment's purpose to the familiar test that still defines the reach of the amendment's protection, asking whether a challenged investigative technique intrudes upon a person's reasonable expectation of privacy.[11] If it does, it is a "search" subject to the Fourth Amendment's requirement that it be reasonable; if it does not, it is not a "search," leaving the police free to employ that mode of investigation without any justification at all. In this essay, I argue that this privacy-based test has led us astray, offering inevitably shrinking protection in our digital world where the line between what

---

[4] *E.g.*, New York City Police Department Public Security Privacy Guidelines (Apr. 2, 2009) (available at http://www.nyc.gov/html/nypd/downloads/pdf/crime_prevention/public_security_privacy_guidelines.pdf).

[5] The Fourth Amendment provides:

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

U.S. CONST. amend. IV.

[6] A few courts have analyzed some modes of electronic surveillance as "seizures," *see, e.g.*, Commonwealth v. Connolly, 454 Mass. 808, 822-824, 913 N.E.2d 356, 396-370 (2009) (holding, under the state Fourth Amendment analog, that police installation and monitoring of GPS device on defendant's vehicle constituted a seizure of the vehicle), but most courts have rejected that construction of the word "seizure," reasoning that, if a mode of surveillance is subject to Fourth Amendment coverage, it is because it is a "search." *See, e.g.*, United States v. Garcia, 474 F.3d 994, 996 (7th Cir. 2007) (observing that, by attaching a GPS to an automobile and then monitoring it, the police "did not 'seize' the car in any intelligible sense of the word").

[7] 277 U.S. 438, 48 S.Ct. 564 (1928).

[8] *See, e.g.*, Silverman v. United States, 365 U.S. 505, 510-512, 81 S.Ct. 679, 682-683 (1961) (holding that a spike microphone inserted through an exterior wall to detect conversations in an apartment, while not a technical trespass, constituted a search because it intruded into the protected space).

[9] 389 U.S. 347, 88 S.Ct. 507 (1967).

[10] *Id*. at 351, 88 S.Ct. at 511.

[11] *Id*. at 361, 88 S.Ct. at 516.

is private and what is public is rapidly disappearing. Said another way, *Katz* has created a trap, putting Fourth Amendment protection at the mercy of technological advances instead of the other way around.

What, then, ought to mark the normative bounds of Fourth Amendment protection? I suggest a return to the amendment's text, not as a way to cabin its reach to that which the framers might have intended or imagined over 200 years ago, but as the appropriate and enduring measure of its reach. The amendment should apply, I argue, to any governmental search, that is, any investigative technique aimed at gathering information, without regard to whether the targeted information is in some sense public and thus not private. Only this approach will ensure that, as technology continues to evolve, the amendment maintains its appropriate normative force, i.e., protecting the people against unreasonable governmental surveillance. This approach would almost certainly broaden the amendment's coverage, requiring the re-thinking of how we decide what is reasonable. But whatever the challenges, one thing is clear – in today's digital world, we cannot intelligibly balance the government's need to investigate and prevent crimes against the people's right to be free from investigative overreach unless surveillance, all surveillance, is subject to this Fourth Amendment calculus.

My argument has four parts.

First, I take a quick look at *Katz*'s privacy-based approach to Fourth Amendment coverage, surveying the journey from its hopeful beginning to the apparent dead-end at which now find ourselves.

Second, I examine the three 21st century cases, *Kyllo*,[12] *Quon*,[13] and *Jones*,[14] in which the Supreme Court has wrestled with the application of the *Katz* test to surveillance involving some form of advanced technology. These cases demonstrate the shortcomings of using privacy to measure Fourth Amendment coverage but offer no solution.

Third, I argue that *Katz* has run its course. Rather than trying to cobble together a fix to its privacy-based test of Fourth Amendment coverage, we should return to the amendment's text, interpreting "searches" to include all investigative techniques aimed at gathering information, thus subjecting all governmental surveillance to the amendment's reasonableness mandate. Indeed, I suggest that the Court may already be doing this, in effect employing the *Katz* reasonable-expectation-of-privacy test not as a measure of Fourth Amendment coverage but instead as a threshold test of reasonableness, sorting out those less intrusive searches that are per se reasonable from those that are sufficiently intrusive to require particular justification, presumptively a warrant. A sort of Fourth Amendment triage. This, I argue, is at best a clumsy, inapt way to deal with the difficult issues raised by modern surveillance; at worst, it is a

[12] Kyllo v. United States, 533 U.S. 27, 121 S.Ct. 2038 (2001).
[13] City of Ontario v. Quon, 560 U.S. --, 130 S.Ct. 2919 (2010).
[14] United States v. Jones, 565 U.S. --, 132 S.Ct. 945 (2012).

disingenuous, flawed approach that utilizes the wrong metric in its threshold reasonableness determination. The amendment is not meant to protect privacy as such. The right that the Fourth Amendment protects is the right to be free from unreasonable governmental intrusions into our personal affairs, without regard to whether our personal information might somehow be public, not private.

Finally, recognizing that my suggested approach will expand the reach of the Fourth Amendment, I offer some tentative thoughts, as well as cautions, concerning the impact of this expansion on the presumption that to be reasonable, a search must be supported by a warrant. This is a very complex issue, fraught with potential danger, and a full analysis of this question is well beyond the scope of this article.

The Privacy-Based Approach to Fourth Amendment Coverage

As noted, *Katz* itself was the 20th century's answer to the how the Fourth Amendment applies to new technology, there electronic monitoring of telephone conversations. Prior to *Katz*, the Supreme Court had taken a trespassory, property-based view of Fourth Amendment coverage, insisting that to be a search, a mode of surveillance had to physically intrude into a protected area. This approach exempted wiretaps from Fourth Amendment coverage.[15] In *Katz*, the police had attached a microphone to the top of a phone booth and listened in on Katz's end of telephone conversations on the pay phone in that booth. Although the case was relatively easy as the law then stood – the microphone sat on, but did not physically intrude into, the phone booth – the Court sought to chart a new course, one not dependent on property concepts, announcing that "the Fourth Amendment protects people, not places."[16] As welcome as this conceptual pivot may have been, its implementation – the now-familiar reasonable-expectation-of-privacy test announced by Justice Harlan in his concurrence – carried the seeds of its own destruction.

First, in his majority opinion Justice Stewart went out of his way to say that the Fourth Amendment does not establish a general right of privacy, stating that while privacy is an important consideration, the amendment in many applications goes beyond privacy protection.[17] However, the operative rule formulated by Justice Harlan was explicitly grounded in privacy, requiring both an actual and "reasonable" expectation of privacy as a predicate for protection.

Second, while it later became clear that this "reasonable expectation of privacy" was intended as a normative expectation,[18] it was far from clear what principles should guide the Court in shaping its contours and then applying it. Mindful of the trap of circularity – that is, a

[15] *Compare* Olmstead v. United States, 277 U.S. 438, 464-66, 48 S.Ct. 564, 568 (1928) (holding a wiretap was not a search because there was no physical intrusion into the house) *with* Silverman v. United States, 365 U.S. 505, 510-12, 81 S.Ct. 679, 682-683 (1961) (holding physical intrusion into apartment, a spike microphone inserted through an exterior wall, constituted a search even though it intruded less than an inch).
[16] Katz, 389 U.S. at 351, 88 S.Ct. at 511.
[17] Katz, 389 U.S. at 350, 88 S.Ct. at 510.
[18] *See, e.g.,* Smith v. Maryland, 442 U.S. 735, 740, 99 S.Ct. 2577, 2580 (1979).

"reasonable expectation of privacy" has to be something other than what the justices, without more, proclaim to be reasonable or legitimate – the Court has on many occasions stated that it looks outside the Fourth Amendment in making this normative judgment.[19] Again a good idea. But, perhaps inevitably, when the cases get decided, that outside source often seems little more than the intuitive judgment of the Court concerning the way the world works, or at least ought to work.

Third, at the same time the Court in *Katz* appeared to chart a new course in defining the reach of the amendment, it hardened its commitment to the presumption of a warrant with its requirement of probable cause as the definition of "reasonable," the substantive measure of Fourth Amendment protection. Although facially adding to the protection provided by the amendment, as it worked out, this warrant presumption may well have hobbled the development of Fourth Amendment protection. Over the years, as the Court applied the *Katz* test to determine the amendment's reach, it plainly has been mindful that to hold that a particular surveillance technique is a search will presumptively require a warrant (or at least probable cause) to satisfy the amendment's requirement that the search be reasonable.[20] Indeed, as one surveys the Court's application of the *Katz* test over the years, it seems increasingly driven by the doctrinal rigidity of the warrant presumption.

Consider these examples, roughly categorized by the kind of information sought.

1. Information Exposed to a Third Party

In *United States v. Miller*,[21] the Court held that grand-jury subpoenas requiring a bank to hand over a person's financial records were not Fourth Amendment searches because the bank customer voluntarily conveyed that financial information to bank employees and thus had no reasonable expectation of privacy in it.[22] That the customer had to disclose this quintessentially private information to the bank in order to use the bank's services, that the information was disclosed for a quite limited purpose (and perhaps with the understanding that it was otherwise confidential), and that the federal Bank Secrecy Act[23] required the bank to keep those records, were all quite beside the point. Using a similar third-party-exposure theory, in *Smith v. Maryland*,[24] the Court held that installing a pen register at the telephone company and using it to learn the telephone numbers called from a private telephone was not a search because the numbers called were revealed – necessarily to be sure – to a third party (the phone company) and thus were not private.[25]

---

[19] *See, e.g.,* Minnesota v. Carter, 525 U.S. 83, 88, 119 S.Ct. 469, 472 (1998).
[20] *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 32, 121 S.Ct. 2038, 2042 (2001).
[21] 425 U.S. 435, 96 S.Ct. 1619 (1976).
[22] *Id*. at 443, 96 S.Ct. at 1624.
[23] Pub. L. No. 91-508, Stat. 1114-1124 (1970) (codified in 12 U.S.C. §§ 1951-1959).
[24] 442 U.S. 735, 99 S.Ct. 2577 (1979).
[25] *Id*. at 743-45, 99 S.Ct. at 2582.

Smith is still good law, and it would seem to exclude from Fourth Amendment coverage much if not all of the National Security Agency's collection of so-called metadata, e.g., records of phone calls (showing the date, time and duration of the calls; the phone numbers, and oft-times the locations, of the callers and those called),[26] credit-card transactions (showing what one bought; when, where and from whom one bought it; how much one paid for it) and the like. Such metadata – all (as was so in *Smith*) disclosed to service providers; none involving the content of any communications[27] – are, in the words of one privacy advocate, "often more significant than the communications [themselves]."[28]

2. Information Exposed to the Public

In *United States v. Knotts*,[29] the Court held that putting a beeper into container of chloroform (used in manufacturing illicit drugs), selling it undercover to a drug suspect and then monitoring the beeper to track the suspect's movements as he traveled over 100 miles through two states to a remote cabin in the woods was not a search because there was no reasonable expectation of privacy in travel upon public roads. The Court reasoned that the suspect had knowingly exposed his whereabouts to anyone who happened to be on or next to the highway, no matter how circuitous or remote his route, and his movements were thus public information.[30] This was so even though the officers themselves needed the beeper to keep track of the suspect.[31] A different sort of public exposure was involved in *California v. Greenwood*,[32] a case in which the Court held that ripping open an opaque bag of trash, left at the curb for trash collection, and rummaging through its contents was somehow not a search. The Court's rationale was that a garbage bag at the curb was exposed to raccoons, snoops, children and other noxious beasts who

[26] This, indeed, is basis for the Obama Administration's claim that "[a] Section 215 [of the USA PATRIOT Act] order for the production of telephony metadata is not a 'search' as to any individual." *See* ADMINISTRATION WHITE PAPER BULK COLLECTION OF TELEPHONY METADATA UNDER SECTION 215 OF THE USA PATRIOT ACT, August 9, 2013, at 19 (available at http://info.publicintelligence.net/DoJ-NSABulkCollection.pdf.)

[27] *See* Peter Baker & David Sanger, *Obama Defends Mining of Data*, N.Y. Times, June 8, 2013, at A11 (quoting President Obama's response to criticisms of this surveillance program, the president saying, "Nobody is listening to your telephone calls. … that is not what this program is about."); James Risen & Eric Lichtblau, *How the U.S. Uses Technology to Mine Data More Quickly*, N.Y. Times, June 9, 2013, at 1, 11 (describing the information collected and its analysis); Hendrick Hertzberg, *Snoop Scoops*, The New Yorker, June 24, 2013, at 3 (describing the information collected) (available at www.newyorker.com/talk/2013/130624taco_talk_hetrzberg).

[28] Marc Rotenberg, Executive Director of the Electronic Privacy Information Center, quoted in James Risen & Eric Lichtblau, *How the U.S. Uses Technology to Mine Data More Quickly*, N.Y. Times, June 9, 2013, at 11. Mr. Rotenberg may well be correct in his assessment of the importance of such data, but, at least as matters now stand, he seems guilty of wishful thinking when he goes on to conclude that "It is a bit of a fantasy to think that the government can seize so much information without implicating the Fourth Amendment interests of American citizens." *Id*. Under *Smith*, that fantasy is reality.

[29] 460 U.S. 276, 103 S.Ct. 1081 (1983).

[30] *Id*. at 281-285, 103 S.Ct. at 1085-1087.

[31] *Id*. at 278, 103 S.Ct. 1083.

[32] 486 U.S. 35, 108 S.Ct. 1625 (1988).

might tear it open, revealing its contents for all to see.[33] As such, any expectation by the bag's owner that its contents would remain free from public scrutiny was not reasonable. Well, maybe.

3. Information Obtained by Aerial Surveillance

In *California v. Ciraolo*,[34] the Court held that even though a homeowner had enclosed his patio in not one, but two, privacy fences (one seven feet tall, one ten feet tall), he did not have a reasonable expectation of privacy in that patio, at least when observed by a police-surveillance aircraft – a precursor to a drone, I suppose. After all, the Court reasoned, the air above that patio was navigable space open to the public, and anyone in an overflying aircraft could see what the police saw from theirs.[35] In a companion case, *Dow Chemical Co. v. United States*,[36] the Court held that aerial photographs of a secure area surrounding an industrial facility were not searches even though a sophisticated mapping camera was necessary to reveal the detailed images revealed in the photos.[37] Here, the Court reasoned that, despite the factory owner's considerable – and largely successful – efforts to keep unwelcome intruders out of its enclosed industrial complex, this secure area was akin to open fields[38] and thus open to aerial observation by those in "public airspace … sufficiently near the area for the reach of cameras."[39]

4. Information Shared with a "False Friend"

In *Hoffa v. United States*,[40] a case that preceded *Katz* by a few months, the Court held that employing an undercover informant to converse with a suspect in the suspect's hotel suite was not a search. According to the Court, the suspect had assumed the risk that his fellow conversationalist would reveal that conversation to others, and he thus could claim no Fourth Amendment protection for what he said.[41] In *United States v. White*,[42] a case that caused Justice

[33] *Id*. at 40-41; 108 S.Ct. 1628-1629.
[34] 476 U.S. 207, 106 S.Ct. 1809 (1986).
[35] *Id*. at 213-214, 106 S.Ct. 1813. Three years later, the Court took a slight step back in *Florida v. Riley*, 488 U.S. 445, 109 S.Ct. 683 (1989). In *Riley*, the Court held that backyard surveillance of a greenhouse by a police helicopter hovering at 400 feet was not a search because it did not intrude upon any reasonable expectation of privacy, *id*. at 450-451, 109 S.Ct. at 697, but Justice O'Connor, whose concurrence provided the necessary fifth vote, opined that the reasonableness of the privacy expectation depended not on what FAA regulations permitted but what was the ordinary practice of private helicopter pilots. If the public ordinarily hovered above Mr. Riley's greenhouse at 400 feet, so, too, could the police without violating his reasonable expectation of privacy; if not, then this surveillance did intrude upon his reasonable expectation of privacy and thus constituted a Fourth Amendment search. *Id*. at 454-455, 109 S.Ct. at 698-699 (O'Connor, J., concurring).
[36] 476 U.S. 227, 106 S.Ct. 1819 (1986).
[37] *Id*. at 238 & n. 5, 106 S.Ct.at 1827 & n. 5.
[38] *See* Oliver v. United States, 466 U.S. 170, 176, 104 S.Ct. 1735, 1740 (1984) (holding that trespassing on privately owned, fenced open fields is not a search); Hester v. United States, 265 U.S. 57, 59, 44 S.Ct. 445, 446 (1924) (same).
[39] Dow Chemical Co., 476 U.S. at 239, 106 S.Ct. at 1827.
[40] 385 U.S. 293, 87 S.Ct. 408 (1967).
[41] *Id*. at 302-303, 87 S.Ct. at 413-414.
[42] 401 U.S. 745, 91 S.Ct. 1122 (1971).

Harlan himself to cry foul,[43] the Court relied on *Katz* to reaffirm this false-friend approach to the contents of ostensibly private conversations, indeed, going beyond *Hoffa* to hold that attaching a wire to the informant to allow agents to listen in on a suspect's conversations in his own home was not a search. The Court reasoned that people assume the risk that someone to whom one says something, no matter where that occurs or what is said, might be a wired informant transmitting that conversation to the police.[44] If we did not know that before *White*, we certainly do after.

Each of these holdings, and others like them, facially rest on the notion that the subjects' respective expectations of privacy – in the bank records, in the telephone numbers called, in the movements of one's car, in the bagged trash, in the fenced patio, in the conversation with a supposed friend – were not reasonable. These judgments, ostensibly grounded in common societal understandings (what one commentator has called empiricism without empirics[45]), are normative, insulating particular investigative techniques from judicial scrutiny concerning their reasonableness under the Fourth Amendment.

It could be that these normative judgments are what they purport to be: objective measures (however questionable one or another may be) of how people view particular claims of privacy. When we put out our trash, we understand that there is a good chance someone or something will rip open the bag, exposing its contents for the world to see; when we open and maintain a bank account, we take the risk that bank employees will reveal to others the personal financial information that we necessarily convey to them and that federal law requires them to keep; and so forth. Because we have a common understanding that such information is not really private, police intrusions to discover it are not investigative techniques about which we should be concerned. But just gauging from the reactions of my students over the past 30 years, if the *Katz* test is really an empirical measure of societal attitudes, the Court is astonishingly tone deaf in many of these judgments. A darker view is that this is faux empiricism, pretending to ground in sources outside the Fourth Amendment the Court's own judgment that particular privacy interests are not worthy of Fourth Amendment protection. Justice Scalia has on occasion taken this more cynical view of the *Katz* test, noting in his concurrence in *Minnesota v. Carter*[46] what he called the "uncanny resemblance" of society's reasonable expectations of privacy to the views of the sitting justices.[47]

---

[43] *Id*. at 786, 91 S.Ct. at 1143 (Harlan, J. dissenting)(arguing that the question was not whether the suspect had assumed the risk that his false friend was wearing a wire, but whether, through intrusions by governmental agents, "we should impose on our citizens the risks of the electronic listener or observer without at least the protection of a warrant requirement").

[44] *Id*. at 751-753, 91 S.Ct. at 1126.

[45] *See* Stephen Henderson, *After United States v. Jones, After the Fourth Amendment Third Party Doctrine*, N.C. J. L. & Tech (symposium edition) at 6 (forthcoming 2013).

[46] 525 U.S. 83, 97, 119 S.Ct. 469, 477 (1998)

[47] *Id*. at 97, 119 S.Ct. at 477 (Scalia, J., concurring). *See* United States v. Jones, 565 U.S. --, --, 132 S.Ct. 945, 962 (2012) (Alito, J., concurring) (conceding the potential for this "degree of circularity" in the *Katz* expectation-of-privacy test).

As problematic as these concerns concerning the *Katz* approach may seem, they may be cosmetic compared to what the future might hold. The *Katz* privacy test may, on occasion, have come up short in protecting people, not places, but at least it seemed a defensible way to think about Fourth Amendment values in the face of emerging 20th century technology – wiretaps, microphones that allowed listening through walls, airplanes that permitted aerial over-flight, beepers that permitted crude tracking of public travel. The Court may not have gotten it right in assessing particular intrusions, but at least Justice Harlan's notion that privacy – a settled concept – lay at the heart of the matter seemed right. That no longer is so. Today's (not to mention tomorrow's) technology has put expectations of privacy in flux, if not threatening privacy altogether. As such, using a privacy-based test to establish the reach of Fourth Amendment protection is not just outmoded; it risks stripping away our constitutional protection against over-reaching governmental surveillance. If that sounds hyperbolic, consider the evidence.

Kyllo, *Quon*, and *Jones*: The Shortcomings of *Katz* Laid Bare

The Supreme Court has certainly been aware of technology's impact on privacy and thus on the *Katz* test,[48] yet the justices have not rushed to fill the gap. Even though surveillance technology has exploded since the turn of the 21st century – roughly the beginning of the so-called digital age[49] – the Court has confronted its impact on Fourth Amendment coverage in only three cases. Moreover, only in the first of these cases, *Kyllo v. United States*,[50] did the Court apply the *Katz* test to decide the amendment's reach. In the latter two, the Court avoided the *Katz* issue, exhibiting open discomfort with its privacy-based test.

Kyllo, the first case, involved thermal imaging of a home, a relatively crude technology by which the police scanned the roof of a house and measured its infrared emissions, thereby determining that one part of the roof was significantly warmer than the rest. This temperature differential suggested that there was indoor plant cultivation in the house, and that information played an essential role in the issuance of a search warrant that uncovered a marijuana-grow operation. The validity of the warrant thus depended on the lawfulness of the warrantless thermal scan. If the scan was a search, it (and the warrant) would be unlawful under the Fourth Amendment, because the scan was conducted without a warrant. If the scan was not a search,

---

[48] As Justice Scalia put it, writing for the Court in *Kyllo v.United States*, 533 U.S. 27, 121 S.Ct. 2038 (2001), the first of the Court's digital-age encounters with technological surveillance, there a thermal scan of a house:

> It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology. … The question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy.

Id. at 33-34, 121 S.Ct. 2043.

[49] *See* ERIC SCHMIDT & JARED COHEN, THE NEW DIGITAL AGE 4 (2013) ("In the first decade of the twenty-first century the number of people connected to the Internet worldwide increased from 350 million to more than 2 billion. In the same period, the number of mobile-phone subscribers rose from 750 million to well over 5 billion (it is now over 6 billion)").

[50] 533 U.S. 27, 121 S.Ct. 2038 (2001).

the Fourth Amendment and its warrant requirement would not apply, and the warrant would stand. All depended on whether the thermal scan was a Fourth Amendment search.

In deciding this question, the Court applied the two-pronged *Katz* test, deciding that Kyllo had both an actual and reasonable expectation of privacy in the information that the thermal scan revealed and thus that the scan constituted a Fourth Amendment search which was unlawful in the absence of a warrant.[51] Although Justice Scalia's majority opinion was a full-throated affirmation of core Fourth Amendment values in the face of emergent technology, the Court qualified this protection by limiting it to technological surveillance through use of "a device not in general public use."[52] This followed from *Katz*.[53] Once people generally can use thermal scanners to enhance their vision and thus see the temperature of your roof, you cannot reasonably complain if the police see what others see; that information, as an objective matter, is no longer private.

It took only 12 years for technology to close the gap, apparently eviscerating *Kyllo*'s Fourth Amendment protection. A "Professional Infrared Thermometer," advertised as capable of detecting surface temperatures up to 3272° F on a one-foot-square area up to 100 feet away, is now commercially available.[54] Its advertised cost is $800, not a pittance to be sure but far less expensive than the "conventional" $22,000 mapping camera used to "enhance somewhat" the vision of the EPA photographer at 12,000 feet in *Dow Chemical Co*.[55] If a sophisticated, expensive mapping camera such as the government used in its surveillance of Dow was in general public use, thus disqualifying the resulting aerial photographs as Fourth Amendment searches under *Katz*, so, too, are advertised $800 infrared scanners, thus disqualifying thermal scans as Fourth Amendment searches. For all of Justice Scalia's bark,[56] *Kyllo*'s Fourth Amendment protection turns out to have little bite.

---

[51] *Id*. at 40, 121 S.Ct. at 2046.
[52] *Id*.
[53] In Justice Stewart's words, "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." Katz, 389 U.S. at 351, 88 S.Ct. at 511. This idea that the constable should not be required to ignore what all can see has roots tracing back to 18th century tort law, holding that the policeman's eye can commit no trespass. *See* Boyd v. United States, 116 U.S. 616, 628, 6 S.Ct. 524 (1886) (cited by Justice Scalia and quoting *Entick v. Carrington*, 19 How. St. 1029, 95 Eng. Rep. 807 (K.B. 1765)). It applies even when the policeman's vision is enhanced, as long as the mode of that enhancement is generally available. *See* Dow Chemical Co. v. United States, 476 U.S. 227, 238, 106 S.Ct. 1819, 1827 (1986) (holding that photographs revealing detail as small as one-half inch in diameter, taken by a sophisticated but publicly available mapping camera at altitudes up to 12,000 feet, did not constitute a search, observing that "[t]he mere fact that human vision is enhanced somewhat, at least to the degree here, do not give rise to constitutional problems").
[54] *See* http://www.thermoworks.com/products/probe. The Supreme Court over-ruled by Costco, where, as of June 1, 2013, a less sophisticated and far less expensive infrared thermometer was on the shelf, available for purchase and use by the general public.
[55] *See supra* note 53; Dow Chemical Co., 476 U.S. at 242 n. 4, 106 S.Ct. at 1829 n. 4 (Powell, J., concurring in part, dissenting in part) (noting the price and high-performance capabilities of the camera).
[56] In framing the issue, Justice Scalia stated, "The question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy." Kyllo, 533 U.S. at 33-34, 121 S.Ct. at 2043. He underscored this point, declaring that "the rule we adopt must take account of more sophisticated systems [of

In the second case, *City of Ontario v. Quon*,[57] open cracks emerged in the Court's confidence in *Katz* as an apt measure of Fourth Amendment coverage. *Quon* involved a police-department supervisor's selective retrieval and reading of a police officer's private text messages from an electronic mobile device that the police department had issued to the officer for use in his police work. The city had explicitly reserved the right to audit the messages but informally had said it would not do so if the employee paid for any overage, which the officer had done. To determine whether reading the officer's private text messages in spite of this assurance constituted a search, *Katz* required the Court to assess society's privacy expectations in text messages sent and received on an employer's mobile device. Eight justices threw up their hands, noting that while in *Katz* their counterparts may have felt comfortable using their own experience to assess the privacy interest in a telephone booth, they felt no such confidence in this world of texting at the office.[58] After discussing at some length the perils of deciding this issue before settled societal privacy expectations in this context had emerged, the Court decided to leave the matter for further fermentation, holding that even if such surveillance constituted a search, it was reasonable.[59]

The Court's discomfort with the *Katz* test continued in *United States v. Jones*,[60] the most recent of these three cases. There, the Court was asked to decide whether, by attaching a GPS device to Jones's car and then monitoring it to determine and record the car's every movement for a month, the police had engaged in a search under the Fourth Amendment.[61] Under *Katz*, the answer would lie in whether such surveillance intruded upon the suspect's reasonable expectation of privacy, a question that the Court again side-stepped. Writing for a four-judge plurality, joined on this point by Justice Sotomayor in her concurrence, Justice Scalia seemed to turn back the clock, resurrecting the trespass-to-property approach that *Katz* was thought to have put to rest. The Court held that attaching the GPS device to Jones's car and monitoring it to determine the car's movements was a trespassory intrusion upon private property for the purpose of obtaining information, which constituted a "search."[62] Since this search was of Jones's car, an

---

surveillance] that are already in use or in development." *Id*. at 36, 121 S.Ct. 2044. When the government argued that room temperature, revealed by infra-red scanning, is not a matter implicating privacy interests, Justice Scalia responded, "In the home … *all* details are intimate details, because the entire area is held safe from prying government eyes." *Id*. at 37, 121 S.Ct. at 2045 (emphasis in original). He concluded:

> [T]he Fourth Amendment draws 'a firm line at the entrance to the house.' That line, we think, must be not only firm but also bright – which requires clear specification of those methods of surveillance that require a warrant. While it is certainly possible to conclude from the videotape of the thermal imaging that occurred in this case that no 'significant' compromise of the homeowner's privacy has occurred, we must take the long view, from the original meaning of the Fourth Amendment forward.

Id. at 40, 121 S.Ct. at 2046 (citation omitted). That firm, bright line of protection against technological advances in surveillance, drawn at the home's threshold and dictated by the "long view," seems to have lasted just 12 years.

[57] 560 U.S. --, 130 S.Ct. 2919 (2010).

[58] *Id*. at --, 130 S.Ct. 2630-2631.

[59] *Id*. at --, 130 S.Ct. at 2632-2633.

[60] 565 U.S. --, 132 S.Ct. 945 (2012).

[61] *Id*. at --, 132 S.Ct. at 949.

[62] *Id*. at -- & n.3, 132 S.Ct. at 950 & n. 3 (2012).

"effect," it was covered by the Fourth Amendment and was thus unlawful in the absence of a valid search warrant.[63]

In reaching this result, Justice Scalia explained that the *Katz* test of Fourth Amendment coverage augmented but did not replace original understandings concerning the amendment's reach, which includes physical intrusions into constitutionally protected areas by the government in order to obtain information. Whether or not this was a fair statement of Fourth Amendment doctrine, such a property-based approach covers only a narrow slice of electronic, particularly digital, surveillance. If the GPS device in *Jones* had been built into the car (as opposed to attached by the police), monitoring the device would not have involved a physical trespass upon Jones's property, leaving it to the *Katz* test to determine if monitoring the GPS, by itself, would have constituted a cognizable Fourth Amendment search. The justices of course understood this point.[64] But, it is one thing to see the problem and quite another to agree on a solution, as the opinions in *Jones* demonstrate. Five justices agreed that *Katz* would yield the same result, but Justice Sotomayor could not bring herself to vote on that basis, leaving the larger *Katz* issue for another day. A closer look at the case justifies Justice Sotomayor's, and with her vote, the Court's reticence.

In *Jones*, a joint District of Columbia and FBI narcotics task force came to suspect Antoine Jones of trafficking narcotics. The officers began an extensive surveillance of Jones, including attaching a GPS device to his wife's car, a car that Jones exclusively used. By monitoring that device around the clock for four weeks, the police determined Jones's precise movements during that time and were thus able to connect him with locations and persons that other evidence tied to the narcotics scheme. Although the police had obtained a warrant authorizing the attachment and monitoring of the GPS device, the warrant only authorized its installation in the District of Columbia within ten days of its issuance. The officers attached the device to Jones's car 11 days after the warrant's issuance and in Maryland to boot. So, the government defended the GPS surveillance as a warrantless intrusion, arguing that neither the installation nor the monitoring constituted a search because neither violated Jones's reasonable expectation of privacy.

---

[63] Holding that the warrantless tracking was unlawful, the Court explicitly declined to address the government's fallback argument that, because its attachment and monitoring of the GPS device was based on reasonable suspicion, indeed probable cause, it was reasonable under the Fourth Amendment. The argument was not raised below, and the Court thus considered it forfeited. *Id*. at --, 132 S.Ct. at 954.

[64] *See id*. at --, 132 S.Ct. at 954 (Scalia, J., writing for the Court) (noting that surveillance without physical trespass "may be … an unconstitutional invasion of privacy, but the present case does not require us to answer that question"); *id* at --, 132 S.Ct. at 955 (Sotomayor, J., concurring) (noting that "physical intrusion is now unnecessary to many forms of surveillance," including "monitoring … factory- or owner-installed vehicle tracking devices or GPS-enabled smartphones"); *id*. at --, 132 S.Ct. at 961 (Alito, J., dissenting) (noting that the Court's reasoning does not apply to long-term monitoring without technical trespass, as for example, monitoring of a GPS tracking device installed in an automobile by the manufacturer).

Notwithstanding the Orwellian overtones of this argument, the government stood on reasonably firm doctrinal ground. As noted above,[65] in *Knotts*, the Court had held that because public travel was open to public view, there was no reasonable expectation of privacy in one's movements, even if they occurred in remote locations. True, in a footnote in *Knotts*, the Court had reserved on the issue of "dragnet type law enforcement practices,"[66] but as Chief Judge Sentelle put it in his dissent to denying rehearing en banc in *Jones*, if there is zero expectation of privacy in one public trip, then "[t]he sum of an infinite number of zero-value parts is also zero."[67]

There are two responses to this argument under *Katz*, but both have a sort of patchwork feel, neither offering much guidance for its application beyond the facts of *Jones*. First, as an empirical matter, there is a difference between being tracked on a single trip and being tracked around the clock for a month. Such prolonged, uninterrupted surveillance could not, as a practical matter, be accomplished by conventional, visual surveillance, and so most would agree as an objective matter that the intensive, non-stop surveillance provided by GPS tracking is not something we in society expect. In terms of the *Katz* test, we have an objectively reasonable, actual expectation that our public comings and goings, minute-by-minute for weeks on end, are as a practical matter private. As Justice Stewart might have put it, we do not knowingly expose to the public a month's worth of our precise whereabouts.

Turning to the normative prong of *Katz*, whether that expectation of privacy is a "reasonable" or legitimate Fourth Amendment expectation, the detailed pattern of conduct that emerges from such prolonged surveillance reveals a great deal of personal and private information about the person subject to such surveillance – not just where he goes, but by "easy inference," why he goes there – an informational "matrix" which reveals more than the sum of the separate instances of travel it catalogs. We expect that this "matrix" of information about the details of how we live is private, and that expectation of privacy is "legitimate." It is thus protected by the Fourth Amendment. Put more succinctly by Judge Wood in her dissent to a Seventh Circuit case holding that GPS monitoring was not a search, *United States v. Cuevas-Perez*,[68] such a surveillance technique is "Orwell[ian],"[69] or by Chief Judge Kozinski in his dissent from denial of rehearing en banc in a similar Ninth Circuit case, *United States v. Pineda-Moreno*,[70] "creepy and un-American."[71]

---

[65] *See supra* notes 29-30 & text.
[66] United States v. Knotts, 460 U.S. 276, 284, 103 S.Ct. 1081, 1086 (1983).
[67] United States v. Jones, 625 F.3d 766, 769 (2010) (Sentelle, C.J., dissenting from denial of rehearing en banc), *rev*., 565 U.S. --, 132 U.S. 945 (2012).
[68] 640 F.3d 272 (7th Cir. 2011).
[69] *Id*. at 286 (Wood, J., dissenting) ("[GPS surveillance] make[s] the system that George Orwell depicted in his famous novel, *1984*, seem clumsy and easily avoidable by comparison").
[70] 617 F.3d 1120 (9th Cir. 2010).
[71] *Id*. at 1126 (Kozinski, C.J., dissenting).

Justice Sotomayor took this argument to heart. In her concurrence, she noted that "with increasing regularity" law enforcement will be able, on the cheap, to "enlist[] factory- or owner-installed tracking devices" in cars and in mobile phones to compile, to store and to have ready access to "a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious and sexual associations."[72] She went on to observe that public awareness of such unrestricted, governmental surveillance would "chill[] associational and expressive freedoms"[73] and could "'alter the relationship between citizen and government in a way that is inimical to democratic society.'"[74]

That law enforcement might theoretically be able to gain information concerning a person's whereabouts by conventional surveillance – good old-fashioned eyeballing – was for Justice Sotomayor entirely beside the point in deciding whether under *Katz* the Fourth Amendment applied to such technological surveillance.[75] For her, the potential for arbitrary misuse by the government of such powerful technology raised Fourth Amendment concerns quite apart from the availability of the same information through traditional surveillance. Indeed, she went a step further, suggesting that it is time to reconsider the so-called third-party doctrine under which information disclosed to a third party is deemed exposed to the public and thus not subject to a reasonable expectation of privacy, thereby precluding Fourth Amendment protection. This doctrine, as noted above,[76] provides the conceptual basis under *Katz* for denying Fourth Amendment coverage to, among other things, phone numbers that one dials on one's phone,[77] the records concerning one's finances that banks are required by law to keep,[78] and presumably the phone-record and credit-card metadata collected, analyzed and stored by the National Security Agency.[79] Noting that people, often by necessity, reveal much information about themselves in the course of day-to-day living, Justice Sotomayor deemed this third-party limitation on *Katz* "ill-suited to the digital age."[80] She suggested that information should not be denied Fourth Amendment protection solely because it was disclosed, even voluntarily, to another for some limited purpose.[81]

Nevertheless, reluctant to resolve these "difficult questions" when in her view it was unnecessary to do so,[82] Justice Sotomayor joined Justice Scalia's trespassory approach, thus providing the fifth vote for deciding the case on that narrow basis.

---

[72] Jones, 565 U.S. at --, 132 S.Ct. at 955-56 (Sotomayor, J., concurring).
[73] *Id*. at --, 132 S.Ct. at 956 (Sotomayor, J., concurring).
[74] *Id.* (Sotomayor, J., concurring) (quoting *United States v. Cuevas-Perez*, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).
[75] *Id*.
[76] *See supra* notes 21-28 & text.
[77] Smith, 442 U.S. at 743-45, 99 S.Ct. at 2582.
[78] Miller, 425 U.S. 443, 96 S.Ct. at 1624.
[79] *See supra* notes 25-28 & text.
[80] Jones, 565 U.S. at --, 132 S.Ct. at 957.
[81] *Id*.
[82] *Id*.

In his concurrence, Justice Alito, joined by Justices Breyer, Ginsburg, and Kagan, shed any such reluctance and took on the *Katz* issue. Justice Alito began by dismissing Justice Scalia's trespass-to-chattels approach, arguing that 18th century tort law is an inapt tool to measure the Fourth Amendment's coverage of 21st century surveillance technology.[83] Not only is it inconsistent with *Katz* – which, notwithstanding Justice Scalia's claim to the contrary, had explicitly over-ruled this trespass-based theory[84] – but it also flies in the face of 45 years of case law that followed *Katz*. More to the point, this reversion to the law of trespass as a measure of Fourth Amendment protection has no application to electronic surveillance, which requires no physical intrusion. This, of course, was the very problem that the Court in *Katz* set out to solve.[85]

Justice Alito conceded that *Katz* has its own problems, particularly as applied to digital technology. He began by noting *Katz*'s potential for circularity and the related problem that judges may "confuse their own expectations of privacy with those of the hypothetical reasonable person to which the *Katz* test looks."[86] As noted above, this is not new. What is new, that is, what differentiates the application of *Katz*'s privacy-based test to digital technology, is the direct connection between this technology and societal privacy expectations. As Justice Alito observed, while the *Katz* test assumes what he called a "well-developed and stable set of privacy expectations," in our digital age societal privacy expectations change with technological advances, often at dizzying speed, resulting in periods of flux during which new expectations emerge, only to be replaced by yet newer, and diminished, expectations spawned by the next generation of technology.[87] Citing reports on NPR and in Time magazine, he noted the apparent inevitability of this cycle:

> New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable.[88]

Even assuming that at any given point in time there is a settled body of privacy expectations, in today's world those expectations are increasingly a function of technology, technology which – like it or not – is relentlessly eroding privacy. In short, societal privacy expectations in today's world present both a moving and a shrinking target.

As examples of this phenomenon, Justice Alito cataloged technology that monitors persons' movements, pointing to the ubiquity of closed-circuit video monitoring in some

---

[83] *Id*. at --, 132 S.Ct. at 957-58 (Alito, J., concurring).
[84] *See* Katz, 389 U.S. at 353, 88 S.Ct. at 512.
[85] *Id*. at --, 132 S.Ct. at 962.
[86] *Id*. at --, 132 S.Ct. at 962.
[87] *Id*.
[88] *Id*.

places,[89] automatic toll-collection systems such as EZPass that record the movement of automobiles on toll roads, GPS systems built into automobiles to assist roadside service or to track stolen cars, and – what Justice Alito regarded as most significant – cell phones and other mobile devices that permit wireless carriers to track and record the minute-to-minute location of users, whether as a necessary aspect of their operation or as social tools by which users advertise their location to promote interaction with (or sometimes to avoid) other users.[90] And these examples are confined to location trackers; they say nothing about the use of on-line purchasing or of credit cards, both of which reveal what users buy, what they pay for it, and when and where they buy it, not to mention digital social networks such as Facebook, in which users release information that many would consider private.

This list is an incomplete but telling sample of today's technology, technology which is only in its infancy.[91] If today drones are the exclusive province of the military, plans are in the works for a much less expensive version that its developers hope soon to make a feature of everyday life.[92] And it seems only a matter of time before there are surveillance drones so small that they will be unnoticed, even indoors.[93] When that comes to pass, will there be any space in which, as an objective matter, one would reasonably expect to be free of surveillance? Will technology eventually condition us to accept ubiquitous surveillance? Justice Alito suggested that such concerns about shrinking privacy might spur action by state and federal legislatures, which, he observed, could move more quickly and effectively than could a court to identify privacy threats and to measure public attitudes in order to institute statutory protections that could strike a comprehensive, detailed balance of privacy and public safety (and that could be adjusted as technology progresses).[94] As sensible as that seems, neither Congress nor the various state legislatures has shown much appetite for such a legislative solution.[95]

---

[89] If it is ubiquitous in some locations in the United States, China – where, in addition to 20-plus million government surveillance cameras, there is a proliferation of private surveillance cameras and electronic listening devices enabling Chinese citizens to spy on each other – may well point the way of the future. *See* Frank Langfitt, *In China, The Government Isn't the Only Spy Game in Town*, NPR, Jan. 30, 2013 (available at http://www.npr.org/2013/01/30/170563866/in-china-the-government-isn't-the-only-spy-game-in-town.).

[90] *Id*. at --, 132 S.Ct. at 963.

[91] For a more complete and colorful cataloging of available surveillance technology, see Chief Judge Kozinski's list in his *Pinedo-Moreno* dissent. United States v. Pineda-Moreno, 617 F.3d 1120, 1124-26 (2010) (Kozinski, C.J., dissenting).

[92] *See* Matthew Wald, *Domestic Drones on Patrol*, N.Y. Times, Mar. 18, 2013, at B1(describing University of North Dakota's academic program in unmanned aviation, "preparing for a brave new world in which cheap remote-controlled airplanes will be ubiquitous in civilian airspace").

[93] AeroVironment,Inc., a developer and manufacturer of unmanned aircraft, has announced the development of a fully operational hummingbird-like surveillance drone, flapping wings and all, in a project funded by the Defense Advanced Research Projects Agency. *See* Press Release, AeroVironment, Inc., AeroVironment Develops World's First Fully Operational Life-Size Hummingbird-Like Unmanned Aircraft for DARPA, (Feb. 17, 2011) (available at http://www.avinc.com/resources/press_release/aerovironment_develops_worlds_first_fully_operational_life-sized_hummingbird). Take a look at http://www.youtube.com/watch?v=a8ZbtZqH6Io.

[94] *Id*. at --, 132 S.Ct. at 962-63, 964.

[95] The Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified 18 U.S.C. §§1367, 2232, 2510 -2521, 2701-2710, 3121-3126) (ECPA), places limits on law-enforcement access to then-extant

Left with that reality, Justice Alito grudgingly turned to *Katz*, applying its privacy-based test in a way that all but conceded its shortcomings as a principled measure of Fourth Amendment coverage of electronic surveillance. Justice Alito opined that the month-long, around-the-clock GPS surveillance in *Jones* intruded on a reasonable expectation of privacy, thus making it a "search," in contrast to the one-trip, 100-plus-mile beeper surveillance which the Court in *Knotts* held was not. He offered no supporting analysis, simply announcing, as if to say it makes it so, that four weeks of tracking Jones's every vehicular movement "surely crossed" *Katz*'s privacy line.[96] Dismissing the criticism that he did not identify the line's location, or even offer any principled way to find it, Justice Alito said that if uncertainty exists, police could always obtain a search warrant. That blithe assertion is by itself telling, coming from the four justices willing to employ *Katz* to mark the foundational, protective boundary between the government and its citizens in this context. If that were not enough, Justice Alito added further uncertainty, suggesting that investigations involving "extraordinary offenses" may well be subject to a different set of reasonable privacy expectations,[97] a different line (if any line at all).

It may be that Justice Alito is an unenthusiastic, unworthy champion of the *Katz* standard, but he identifies serious problems with its approach. The more likely reality is that the standard itself has run its course. As noted above, in her concurrence, Justice Sotomayor seems committed to refurbishing the *Katz* test, suggesting among other possibilities rethinking the

---

electronic communications, but 27 years of technological development – including the advent of the so-called digital age – has opened holes in this statutory protection. There have been attempts to update its protections, but the 9-11 terrorist attacks undercut the political will for such upgrades, indeed, prompting national-security legislation such as the USA PATRIOT Act of 2001, Pub. L. 107-56, 115 Stat. 272 (codified in scattered sections of 8 U.S.C., 15 U.S.C., 18 U.S.C., 22 U.S.C., 31 U.S.C., 49 U.S.C. and 50 U.S.C.), that weakened certain privacy protections against surveillance. *See* Jason Krause, *Prying Eyes*, April 2013 ABA J. 47 (surveying shortcomings of, and attempts to amend, the ECPA). The most recent attempt at an ECPA upgrade was a bill offered in November 2012 by Senator Leahy, Chairman of the Senate Judiciary Committee, to require warrants to gain access to email messages stored on private servers and to track cellphones. *Id*.at 49. Although the proposed amendment enjoyed bi-partisan support, it did not make it to the Senate floor for a vote before the end of the term. *See* Editorial, *Googling You*, N.Y. Times, Mar. 17, 2013, at SR 10.

State legislative efforts have fared no better. For example, the California legislature passed a bill requiring a warrant to gain access to cellphone location records from carriers, but Governor Brown vetoed the bill, saying that it did not strike "'the right balance between the operational needs of law enforcement and individual expectations of privacy.'" *See* Somini Sengupta, *Courts Divided Over Searches of Cellphones*, N.Y. Times, Nov. 26, 2012, at A3. Similarly, the Rhode Island legislature passed legislation requiring a warrant to search a cellphone, but Governor Chafee vetoed it, saying "'The courts, not the legislature, are better suited to resolve these complex and case-specific issues.'" *Id*.

The paucity of legislative efforts to rein in police surveillance can hardly come as a surprise. As Anthony Amsterdam observed over a half-century ago (well before the onset of today's terrorist threats):

> The longtime, wholesale "legislative default" in regulating police practices is no accident. Legislatures have not been, are not now, and are not likely to become sensitive to the concern of protecting persons under investigation by the police. Even if our growing crime rate and its attendant mounting hysteria should level off, there will remain more than enough crime and fear of it in American society to keep our legislatures from the politically suicidal undertaking of police control.

Anthony Amsterdam, *Perspectives on the Fourth Amendment*, 58 Minn. L. Rev. 349, 378-379 (1958).

[96] Jones, 565 U.S. at --, 132 S.Ct. at 964.

[97] *Id*.

third-party doctrine by which sharing information with third parties (e.g., sharing your location with your wireless provider by the wireless signals from your cell phone to the provider) negates your reasonable expectation of privacy in your location, even though this "sharing" is not only technical at best but is necessary to the use of the phone. That would help, but it would do nothing for other technological surveillance, both extant (e.g., video monitoring, perhaps accomplished by drones) and future technologies. It is time to consider a different approach, one that takes us forward by going back to the Fourth Amendment itself.

A Return to Basics: A Search is a Search is a Search[98]

The Fourth Amendment protection is against unreasonable searches and seizures directed at persons, houses, papers and effects, searches conducted by the government.[99] And, as the Court acknowledged in *Kyllo*, the meaning of the word "search" remains pretty much the same today as it did in the 18th century, i.e., " '[t]o look over or through for the purpose of finding something; to explore; to examine by inspection; as, to *search* the house for a book; to *search* the wood for a thief.' "[100] However, in breaking the conceptual, property-based grip of physical trespass on what constitutes a search, the Court in *Katz* and its progeny has become more focused on what is revealed by an intrusion and less on the intrusion itself. *Katz*, certainly Justice Stewart's opinion for the Court, could be read simply to hold that an electronic intrusion, like its physical counterpart, is under the above definition a search (for words spoken) and that a phone booth, during the course of a telephone call, is a place analogous to a house or an effect. Instead, Justice Harlan's privacy-based test has become the analytic center-piece, assessing the privacy interest in what was revealed by an intrusion to decide if the intrusion was a search.

This may not be accidental or happenstance. If, as seems reasonably straightforward, tearing open and sorting through a trash bag is a search – an act by the police to "look through [the bag] for the purpose of finding something" – then the question is, was it reasonable? Under current doctrine, reaffirmed by *Katz*, this reasonableness question would presumptively be answered by requiring a search warrant. Or, if flying over a fenced patio – an act by the police "to examine by inspection" what is in the enclosed area – is a search, again, a warrant is presumptively required to satisfy the Fourth Amendment's reasonableness requirement. And so on. From that perspective, this reverse engineering of *Katz*[101] is understandable. First decide what the privacy interest is before deciding whether to call the intrusion that revealed it a search, because if it is a search, it will be subject to the presumptive warrant requirement. In effect, this

---

[98] With apologies to Gertrude Stein, *Sacred Emily* (1913), appearing in GEOGRAPHY AND PLAYS (1922) ("Rose is a rose is a rose is a rose"). Some things one needs no more than to say. *Cf*. Arizona v. Hicks, 480 U.S. 321, 325, 107 S.Ct. 1149, 1153 (1987) (in holding that an officer's moving of a stereo turntable to see its serial number constituted a search, Justice Scalia intoned, "A search is a search, even if it happens to disclose nothing but the bottom of a turntable.").

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

[100] Kyllo, 533 U.S. at 32 n. 1, 121 S.Ct. at 2043 n. 1 (quoting NOAH WEBSTER, AN AMERICAN DICTIONARY OF THE ENGLISH LANGUAGE 66 (1828) (reprint 6th ed. 1989)).

[101] *Id*. at 32, 121 S.Ct. at 2042.

approach implements a two-stage reasonableness inquiry. If the privacy interest revealed by a particular kind of search is relatively slight, the search is deemed presumptively reasonable by employing the legal fiction that it is not a search at all, thus avoiding any further reasonableness inquiry under the Fourth Amendment. If, on the other hand, the privacy interest at issue is significant, the Court requires more to satisfy the amendment's reasonableness command, presumptively a warrant.

This take on *Katz* is hardly new. Indeed, the justices themselves have more or less acknowledged it. In *Kyllo*, which as noted above dealt with visual surveillance of a house enhanced by a thermal imaging device, Justice Scalia surveyed the *Katz* landscape, noting that while Fourth Amendment coverage no longer depends on physical trespass, ordinary visual surveillance remains categorically lawful under the Fourth Amendment even though the original theory – that under the laws of England, the eye cannot commit a trespass – no longer seems viable. Justice Scalia noted that while the new theoretical justification for permitting visual "searches" of things in public view would seem to be that they are reasonable, the stated rationale under *Katz* is that they are not searches at all, "perhaps in order to preserve somewhat more intact [the Court's] doctrine that warrantless searches are presumptively unconstitutional."[102] In dissent, Justice Stevens agreed with Justice Scalia's assessment of *Katz*, even if he did not, openly at least, agree with the reason for it. Justice Stevens cast the issue in terms of presumptive reasonableness. He observed that warrantless searches inside a home are presumptively unreasonable but that warrantless searches of "property in plain view are presumptively reasonable," citing among other examples "the search and seizure of garbage left for collection outside the curtilage of a home" (*Greenwood*) and "the aerial surveillance of a fenced-in backyard from the altitude of 1,000 feet" (*Ciraolo*).[103] In this view, each was a search that was presumptively reasonable, apparently due to the Court's assessment of the privacy interests involved.

A somewhat different, but at bottom similar, approach seems at work in ***Bond v. United States***.[104] There, the Court held that under *Katz*, an officer's single squeeze of a canvas travel bag stuffed into the overhead compartment on an inter-state bus constituted a search of the bag. The squeeze revealed what the officer recognized to be a brick-shaped object consistent with bulk cocaine, leading to a further search of the bag, which confirmed that it was indeed cocaine. In arguing that the squeeze did not constitute a search under *Katz*, the government pointed out that, by putting his bag in a position that every bus traveler knows will subject it to the "dog-eat-dog" pushing, pulling, prodding and squeezing by strangers in "a world of travel that is

---

[102] *Id*. *See also* California v. Acevedo, 500 U.S. 565, 583, 111 S.Ct. 1982, 1993 (1991) (Scalia, J., concurring) ("Our intricate body of law regarding 'reasonable expectation of privacy' has been developed largely as a means of creating these exceptions [to the presumptive warrant requirement], enabling a search to be denominated not a Fourth Amendment search and therefore not subject to the general warrant requirement").
[103] Kyllo, 533 U.S. at 42 & n. 2, 121 S.Ct. at 2047-2048 & n. 2 (Stevens, J., dissenting).
[104] 529 U.S. 334, 120 S.Ct. 1462 (2000).

somewhat less gentle than it used to be,"[105] Bond reasonably understood that his bag would be squeezed. He thus had no actual, much less objectively reasonable, expectation of avoiding such a squeeze.

The Court accepted that the suspect expected his bag to be handled, just not in an "exploratory manner."[106] That was enough for the Court. In his dissent, Justice Breyer argued that, except for its purpose – which under Fourth Amendment doctrine cannot be taken into account[107] – the officer's squeeze was indistinguishable from the expected handling of the bag.[108] But the Court apparently decided that such bus surveillance went beyond what was presumptively reasonable and required more to satisfy the Fourth Amendment. Why? It did not say, but it had to be the privacy interests in the general contents of one's luggage.[109] The contents of a garbage bag sitting at the curb for pick-up are not sufficiently private to require Fourth Amendment justification, presumptively a warrant, for the police to rip it open and examine its contents, but the contents of a canvas bag put in the luggage rack of a bus are sufficiently private to require a warrant for the police just to squeeze it in a manner that roughly reveals its contents. Put on a constitutional continuum, the baggage squeeze is more like the thermal scan of a house (at least before infrared thermometers became generally available) than the act of tearing open and rummaging through a trash bag.

And in *Jones*, Justice Alito's analysis is consistent with, even if it does not openly employ, this approach. He compares the "relatively short-term monitoring of a person's movements on public streets" in *Knotts* with "the use of longer term GPS monitoring" in *Jones*, monitoring that "for four weeks … tracked every movement that [Jones] made in the vehicle he was driving." The former was presumptively reasonable as measured against societal expectations of privacy; the latter was not, at least in investigating "most offenses." However, Justice Alito reserved judgment on whether "prolonged GPS monitoring in the context of investigations involving extraordinary offenses would similarly intrude on a constitutionally protected sphere of privacy."[110] It is difficult to understand how the intrusiveness of the same investigative technique on privacy interests could vary depending on the nature of the investigation in which they are employed. Rather, it seems that Justice Alito is introducing the governmental-need side of the interest balancing that informs reasonableness analysis once it is divorced from the warrant presumption. It may well be, as the Court has held in its analysis of seizures, that the reasonableness calculus changes when the investigation involves a serious

[105] *Id*. at 340, 120 S.Ct. at 1466 (Breyer, J., dissenting).
[106] *Id*. at 338-339, 120 S.Ct. at 1465.
[107] *See* Whren v. United States, 517 U.S. 806, 813, 116 S.Ct. 1769, 1774 (1996).
[108] *See* Bond, 529 U.S. at 341-342, 120 S.Ct. at 1466-1467 (Breyer, J., dissenting).
[109] *See* Chadwick v. United States, 433 U.S. 1, 13-16, 97 S.Ct. 2476, 2484-2486 (1977) (holding that because – unlike an automobile – a footlocker is a repository of one's personal effects, a warrant is required to search it).
[110] Jones, 565 U.S. at --, 132 S.Ct. at 964 (Alito, J., concurring).

national security threat or potential catastrophic threat,[111] but that analysis remains hidden, tucked away in the privacy focus of *Katz*.

Why worry, if the Court recognizes that these non-searches are really searches (or even if it wants to pretend, as a legal matter, that they are not searches)? This would hardly be the first legal fiction, and as long as the Court makes the reasonableness determination, what is the difference?

There are several reasons for concern.

First, this two-stage reasonableness inquiry lacks transparency, obscuring the analytic framework by which Fourth Amendment reasonableness is determined. At best, this impedes the development of coherent doctrine; at worst, it permits those with an agenda to do their work behind closed doors.

Second, the first stage of this two-stage reasonableness inquiry – the *Katz* privacy test – is incomplete. To be sure, the privacy interest in question is pertinent concerning whether an intrusion or surveillance technique is reasonable, but that is only half the story. The other side of the reasonableness balance has always been, and must be, the governmental interest served by that search and the necessity of that search to advancing that interest. In analyzing the reasonableness of searches in which the Court has held that the warrant requirement is inapt, e.g., so-called special-needs searches such as public-school searches[112] and drug testing,[113] the Court has always balanced the privacy interest at stake against the government's interest said to justify the search, including examining the need for the search to advancing that interest.[114] Either the

---

[111] *Cf*. Florida v. J.L., 529 U.S. 266, 273-274, 120 S.Ct. 1375, 1380 (2000) (in holding that an anonymous tip that a particular person had a gun, standing alone, did not constitute reasonable suspicion to stop and frisk that person, the Court qualified its holding, stating:

> The facts of this case do not require us to speculate about the circumstances under which the danger alleged in an anonymous tip might be so great as to justify a search even without a showing of reliability. We do not say, for example that a report of a person carrying a bomb need bear the indicia of reliability we demand for the report of a person carrying a firearm before the police can constitutionally conduct a frisk.).

[112] New Jersey v. TLO, 469 U.S. 325, 105 S.Ct. 733 (1985); Safford Unified School Dist. No. 1 v. Redding, 557 U.S. 364, 129 S.Ct. 2633 (2009).

[113] Skinner v. Railway Labor Executives' Assn., 489 U.S. 602, 109 S.Ct. 1402 (1989); National Treasury Employees Union v. Von Raab, 489 U.S. 656, 109 S.Ct. 1384 (1989); Vernonia School Dist. 47J v. Acton, 515 U.S. 646, 115 S.Ct. 2386 (1995); Chandler v. Miller, 520 U.S. 305, 117 S.Ct. 1295 (1997); Ferguson v. City of Charleston, 532 U.S. 67, 121 S.Ct. 1281 (2001); Board of Education of Independent School District No. 92 of Pottawatomie County v. Earls, 536 U.S. 822, 122 S.Ct. 2559 (2002).

[114] For example, in *Vernonia School Dist. 47J v. Acton*, 515 U.S. 646, 115 S.Ct. 2386 (2001), the Court considered the constitutionality of suspicionless, special-needs (i.e., non-law-enforcement) drug testing of public-high-school students participating in interscholastic sports. In analyzing the reasonableness of this program of drug testing, the Court looked first at the privacy interests of the students, examining the information revealed and the manner in which it was extracted, and then balanced those interests against the nature and immediacy of the governmental interests, including the need for the testing program to meet those interests, ultimately concluding that the drug-testing was reasonable under the Fourth Amendment. *See id*. at 654-665, 115 S.Ct. at 2391-2397.

This balancing approach is not confined to special-needs analysis. The existence and scope of exceptions to the warrant requirement have long depended on such interest balancing. *See, e.g.*, Chimel v. California, 395 U.S. 752,

Court is not counting this in its threshold reasonableness calculus or it is assigning it undisclosed weight. The closest a justice has come to openly considering this side of the reasonableness balance in this threshold inquiry is Justice Alito's suggestion that the GPS surveillance in *Jones* might not be a cognizable search, i.e., might be presumptively reasonable, if it is employed in investigating an "extraordinary crime." This would seem to be a valid part of a reasonableness inquiry, but it is all *sub rosa*, hidden away in the *Katz* test.

Third, this meat-axe approach, dividing searches between those that are presumptively reasonable (thus requiring no justification) and those that presumptively require a warrant to be reasonable, is inapt in the digital world. The threshold judgment required by *Katz* depends on a judicial assessment of privacy interests – a cloistered view at best – in a world in which, at dizzying speed, technology is transforming societal notions of privacy, if not eviscerating it altogether. If the justices decide, based on who knows what, that an interest is sufficiently private, then – as matters now stand – they are left with one choice, i.e., a search warrant is presumptively required to satisfy the Fourth Amendment's reasonableness requirement. Surely the various kinds of modern surveillance and the purposes to which they are put do not so neatly fit into one of these two categories. We need a scalpel, not a meat axe.

Finally, and most important, this first-stage assessment of Fourth Amendment reasonableness uses the wrong metric. Societal expectations of privacy, even if the Court were competent at a given point in time to judge them in this fast-changing digital world, cannot be the sole measure of what is reasonable, even as a threshold matter. What objectively we regard as private – information to which others do not have access – is an ever-shrinking slice of our lives. But the fact that one's neighbor, or credit-card company, or banker, or phone service provider might – of necessity or even choice – know something about each of us does not mean that the government should thus have automatic access to that information.

762-768, 89 S.Ct. 2034, 2040-2043 (1969) (balancing the individual's right to privacy in his home against the police officer's need to protect himself from a weapon and potential evidence from destruction, the Court recognized and limited the scope of a warrantless search incident to arrest to the arrestee's person and the area within his immediate control). Indeed, despite protestations to the contrary, the Court employed such balancing to justify suspicionless DNA testing of felony arrestees, the stated purpose of which testing was to determine if those arrested had committed earlier unsolved crimes. *See* Maryland v. King, 569 U.S. --, -- S.Ct.-- Slip Op. No. 12-207 (2013). The testing was accomplished by a buccal swab of the arrestee's inner cheek and subsequent lab analysis of the cells thus gathered. The Court went to great length to characterize the testing program as a means of identifying those arrested, Slip Op. at 10-13, 18-23 (Kennedy, J., for the Court), an administrative rather than a law-enforcement need. However, in his dissent Justice Scalia makes plain the implausibility of that claim, arguing that both on its face and in its operation the testing program was designed to solve unsolved crimes, a pure law-enforcement need. *See* Slip Op. No. 12-207 at 5-17 (Scalia, J., dissenting). Whoever is right about the character of the DNA testing, and Justice Scalia's view seems more persuasive, the Court's holding that such searches are reasonable under the Fourth Amendment openly rests on balancing the arrestee's diminished expectation of privacy implicated by such swabs coupled with the information revealed by subsequent lab analysis, Slip. Op. No. 12-207 at 8-10, 23-26, 26-28 (Kennedy, J.), against the government's interests in the resulting information and the need for such testing to get it. I*d*. at 10-23.

The Fourth Amendment marks a line between the government and its citizens, setting off a citizen's space that should, as a normative matter, be free from unfettered governmental intrusion, surveillance. The concern is not privacy as such but rather the government's ability forcibly or surreptitiously to invade one's personal affairs. Perhaps no one has put it better than Justice Brandeis in his famous *Olmstead* dissent:

> The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the government, the right to be let alone – the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means imposed, must be deemed a violation of the Fourth Amendment.[115]

The limitation which the Fourth Amendment imposes in protecting that right to be let alone, while not absolute, is facially straightforward, protecting us from unreasonable searches and seizures of our persons, houses, papers and effects. We ought to take that seriously. Any government activity the purpose of which is to gather information about its citizens is a search and should thus be subject to the constitutional command that it be reasonable. Period. Surveillance by GPS, by security cameras, by drone aircraft, by everything from old-fashioned eye-ball observation by a cop on the beat to computer-enabled collection of metadata from private sources that have access to it – each is a search; each is subject to the amendment's requirement that it be reasonable.

Plainly, this would be a bigger Fourth Amendment than we have now, and it almost certainly would require re-thinking – or at least re-casting – the interpretive approaches to defining the amendment's reasonableness mandate. What might inform this reasonableness balancing? While, as noted at the outset, it is beyond the scope of this essay to fully consider the expanded reasonableness analysis for which I call, a few points seem worth making.

Fourth Amendment Reasonableness in a post-*Katz* World

The starting point for thinking about the meaning of the Fourth Amendment command that searches be reasonable if "search" includes all governmental investigative activity would be the presumption that to be reasonable, a search must be justified by a warrant. After all, it is this doctrinal mandate that appears to have engendered the two-stage reasonableness approach of *Katz*. On its face, the Fourth Amendment imposes no such requirement. All that the amendment mandates in this regard is that searches and seizures be reasonable. The amendment separately

[115] Olmstead v. United States, 277 U.S. 438, 478, 48 S.Ct. 564, 572 (1928) (Brandeis, J., dissenting).

provides for the issuance of warrants, requiring that they be based on probable cause under oath or affirmation and that they specify with particularity the places to be searched and the items to be seized. These separate textual commands have caused some to argue that interpreting the amendment's categorical reasonableness requirement presumptively in terms of a warrant turns the amendment on its head, allowing the amendment's limitations concerning the issuance of warrants to predominate over its broader, reasonableness command.[116]

Nevertheless, there are good reasons, jurisprudential and historical, that support a warrant preference, certainly where core Fourth Amendment values are at stake.

From a policy perspective, a warrant requirement ensures that searches are justified based on a single, longstanding standard – probable cause; it ensures antecedent justification for searches, based on a neutral magistrate's determination of probable cause; it ensures that the basis for that determination is reduced to writing under oath or affirmation, which provides a record of the basis for that determination, permitting its subsequent review; it ensures that those conducting the search are informed of the particular limits on the scope of that search; it ensures that one subject to such a search is given notice of the authority for and the limits of the search. Taken together, these features of the warrant requirement address the concerns that searches be for a proper purpose, tailored in scope to serve that purpose, and that they not be arbitrary in either their initiation or scope.

As for history, one need look no further than the observations of Felix Frankfurter:

> One cannot wrench "unreasonable searches" from the text and context and historic content of the Fourth Amendment. It was the answer of the Revolutionary statesmen to the evils of searches without warrants and searches

---

[116] Indeed, Telford Taylor makes a compelling argument that the framers of the Fourth Amendment were principally concerned about warranted searches, seeing warrants as the problem which the amendment is designed to cure rather than the answer to a broader concern that searches be reasonable. As Professor Taylor puts it, summarizing the results of his historical inquiry regarding the "original understanding" of the Fourth Amendment:

> [O]ur constitutional fathers were not concerned about warrantless searches, but about overreaching warrants [principally statutorily authorized "writs of assistance," issued by a court and generally authorizing the bearer to enter any place, including houses, to search for and seize "prohibited and uncustomed" goods]. It is perhaps too much to say that they feared the warrant more than the search, but it is plain enough that the warrant was the prime object of their concern. Far from looking at the warrant as a protection against unreasonable searches, they saw it as an authority for unreasonable and oppressive searches, and sought to confine its issuance and execution in line with the stringent requirements applicable to common-law warrants for stolen goods – an interesting use of a practice already obsolescent to limit and mitigate a current and dangerous practice.

TELFORD TAYLOR, TWO STUDIES IN CONSTITUTIONAL INTERPRETATION 41 (Ohio St. U. Press 1969). *See also* AKHIL AMAR, THE CONSTITUTION AND CRIMINAL PROCEDURE, FIRST PRINCIPLES 4 (Yale U. Press 1997) (arguing that reading the Fourth Amendment's two separate commands to provide that "warrants are not required, but any warrant that does issue is per se unreasonable if not supported by probable cause, particular description, and the rest ... squares more snugly with the amendment's specific words, harmonizes better with its historic context, and makes considerably more common sense.").

> with warrants unrestricted in scope. Both were deemed unreasonable. Words must be read with the gloss of the experience of those who framed them.[117]

In spite of the warrant presumption's apparent advantages and pedigree, it is fair to say that over the past century the Court has vacillated in its allegiance to it. For the 50 years that preceded *Katz*, there was open disagreement among the justices concerning the existence of a categorical warrant requirement, some decisions recognizing it, others rejecting it.[118] By the time of *Katz*, however, the presumption had prevailed, at least rhetorically.[119]

But no sooner had the Court recognized the warrant presumption's ascendancy than it began to trim back its force, eventually recognizing a score of exceptions to it, including many that directly impact core Fourth Amendment values. So, for example, the Court has held that the following warrantless searches of one's home are reasonable: the entry and search of a suspected felon's home if he fled into it in response to police pursuit,[120] the entry and search of a home based on consent either by a resident or by a third party who has reasonably apparent authority to give such consent,[121] the search of the area within the immediate control of a person arrested in his home,[122] the protective sweep of an arrestee's home if, in the course of the arrest, officers have a reason to suspect that an armed confederate might be in the home,[123] the entry and search of a home if officers have a reason to suspect that emergency assistance is required,[124] the entry and search of a home for evidence of a crime if officers have probable cause to believe that such evidence is inside the home and have reason to suspect that securing a search warrant would

---

[117] United States v. Rabinowitz, 339 U.S. 56, 69-70, 70 S.Ct. 430, 436 (1950) (Frankfurter, J., dissenting).

[118] *Compare* California v. Acevedo, 500 U.S. 565, 582, 111 S.Ct. 1982, 1992 (1991) (Scalia, J., concurring) (summarizing the Supreme Court's Fourth Amendment decisions as "lurch[ing] back and forth between imposing a categorical warrant requirement and looking to reasonableness alone. (The opinions preferring a warrant involv[ing] searches of structures") *with id*. at 586, 111 S.Ct. at 1994 (Stevens, J., dissenting) (arguing that, particularly after World War II and Justice Jackson's service as a special prosecutor at the Nuremburg trials, the Court had consistently read the Fourth Amendment to impose a presumptive warrant requirement, for reasons of both history and policy).

[119] *See, e.g.,* Katz v. United States, 389 U.S. 347, 357, 88 S.Ct. 507, 514 (1967) ("'Over and again this Court has emphasized that the mandate of the [Fourth] Amendment requires adherence to judicial processes,' and that searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment – subject only to a few specifically established and well-delineated exceptions." (citations omitted)); Chimel v. California, 595 U.S. 752, 761, 89 S.Ct. 2034, 2039 (1969) (recognizing a presumptive warrant requirement and narrowing the scope of the search-incident-to-arrest exception to it); Coolidge v. New Hampshire, 403 U.S. 443, 449, 453, 91 S.Ct. 2022, 2029, 2031 (1971) (recognizing a presumptive warrant requirement in holding that the warranted search of an automobile was unreasonable because the warrant was issued by the state's attorney general and not a neutral magistrate).

[120] Warden, Md. Penitentiary v. Hayden, 387 U.S. 294, 298-299, 87 S.Ct. 1642, 1645 (1967) (decided a little over six months before *Katz*).

[121] Illinois v. Rodriguez, 497 U.S. 177, 181, 185-186, 110 S.Ct. 2793, 2797, 2799-2800 (1990).

[122] Chimel v. California, 595 U.S. 752, 761, 89 S.Ct. 2034, 2039 (1969).

[123] Maryland v. Buie, 494 U.S. 325, 335, 110 S.Ct. 1093, 1099 (1990) (also recognizing authority to search adjacent spaces from which an attack might be launched, whether or not the officer had reasonable suspicion that armed confederates were present).

[124] Brigham City, Utah v. Stuart, 547 U.S. 398, 403-404, 126 S.Ct. 1943, 1947 (2006).

result in the destruction of the evidence,[125] and the entry of a home by a welfare case worker to conduct an inspection as a condition of continued receipt of welfare benefits.[126]

Each of these exceptions to the warrant presumption is based on balancing of individual interests and competing governmental interests implicated by the kind of search in question. Take for example searches of private homes related to fire. A city-wide inspection program to ensure compliance with a city's fire code requires a warrant, but it is an administrative warrant that is less demanding than a traditional warrant.[127] While an administrative warrant must be based on probable cause demonstrated to a neutral official, this version of probable cause does not require that the fire inspector demonstrate individualized suspicion of code non-compliance. Instead, it requires only that the inspector satisfy the issuing official that the inspection of the house in question is part of an administrative inspection program which includes reasonable administrative or legislative standards for conducting such searches.[128] Given the limited privacy intrusion and the public need for such inspection programs to prevent fires,[129] the principal concern in this context is in controlling the inspector's discretion and in providing adequate notice to the homeowner of the inspector's authority to conduct the limited inspection.[130] In effect, this administrative-warrant approach, while preserving facial allegiance to the warrant requirement, marks a departure from it, one that is fashioned to address the particular Fourth Amendment interests there at stake.

On the other hand, if a house is ablaze, fire-fighters need no warrant to enter, forcibly if necessary, to fight the fire.[131] This is no more than an application of the familiar exigent-circumstances exception to the warrant requirement in which the privacy interests in the house yield to the public-safety interest in extinguishing the fire. Fire investigators may remain on the premises without a warrant for a reasonable time after the fire has been extinguished,[132] reflecting the reduced privacy expectations of the occupants and the continuing public-safety interest at that point in ensuring that the fire does not re-ignite and in determining its cause. But once exigency is over and the investigators leave, if the home is in such condition that its occupants retain a reasonable expectation of privacy in it, the fire inspectors need either consent or a warrant to re-enter.[133] An administrative warrant will do if the investigators' interest is to determine the fire's cause and origin, the scope of that search being confined to intrusions

---

[125] Kentucky v. King, 563 U.S.--, --, 131 S.Ct. 1849, 1856 (2011).
[126] Wyman v. James, 400 U.S. 309, 318, 91 S.Ct. 381, 386 (1971).
[127] Camara v. Municipal Ct. of City and County of San Francisco, 387 U.S. 523, 538, 87 S.Ct. 1727, 1735-1736 (1967); Michigan v. Tyler, 436 U.S. 439, 507, 98 S.Ct. 1942, 1949 (1978).
[128] Camara, 387 U.S. at 538, 87 S.Ct. at 1736. Although it imposes a warrant requirement, the Court does not seem to authorize forcible entry of a building even with a warrant in hand. *Id*. at 540, 87 S.Ct. at 1736.
[129] *Id*. at 535-37, 87 S.Ct. at 1734-35.
[130] *Id*. at 532-33, 87 S.Ct. at 1732-33.
[131] Tyler, 436 U.S. at 509, 98 S.Ct. at 1950.
[132] *Id*. at 510, 98 S.Ct. at 1950.
[133] Michigan v. Clifford, 464 U.S. 287, 104 S.Ct. 641 (1984).

necessary to that purpose.[134] If, on the other hand, the purpose of the search is to find and seize evidence of a crime, a traditional warrant based on probable cause is required.[135] Whether or not one agrees with the particular interest balances struck in crafting these exceptions, each of these departures from the traditional warrant requirement depend on balancing the individual's interests – for the most part privacy but also freedom from arbitrary exercise of official discretion – against the competing governmental interests justifying the particular intrusion in question.

While the interest balance for many forms of surveillance might not support the need for a warrant, there is no reason to think that the warrant presumption applicable to entries into homes would change if Fourth Amendment coverage expands to include all investigative techniques. The suggested change certainly broadens what constitutes a search, but physical intrusions into a home have always been regarded as searches, searches that lie at the amendment's core. As to them, the presumptive requirement of warrant would almost certainly remain undisturbed.

In contrast, many forms of surveillance have long been treated as beyond the amendment's reach. Historically, before the 20th century's technology revolution, surveillance basically meant visual or audio observation, perhaps physically enhanced by binoculars or the like. Because Fourth Amendment searches were then defined in terms of property-based notions of trespass, this surveillance remained outside the amendment's coverage under the theory that the eye (and presumably the ear) can commit no trespass.[136] As we have seen, all of that purported to change under *Katz*, which abandoned this trespassory approach to Fourth Amendment coverage,[137] yet visual surveillance – whether naked-eye[138] or enhanced by technology, at least commonly available technology[139] – remains beyond Fourth Amendment regulation, because, depending on how one views *Katz*, such surveillance either is not a search, or it is a search that is presumptively reasonable.[140]

This would of course change if all forms of surveillance, from naked-eye observation to surveillance accomplished by the most sophisticated technology, are recognized as searches. But just because a mode of surveillance is covered by the Fourth Amendment does not mean that the

---

[134] *Id*. at 294, 104 S.Ct. at 647 (to secure such a warrant, the investigators "need only show that a fire of undetermined origin has occurred on the premises, that the scope of the proposed search is reasonable and will not intrude unnecessarily on the fire victim's privacy, and that the search will be executed at a reasonable and convenient time.").
[135] *Id*.
[136] *See supra* note 53.
[137] *But see* Jones, *supra* notes 62-63 & text, resurrecting this approach.
[138] *See* California v. Ciraolo, 476 U.S. 207, 213, 106 S.Ct. 1809, 1812 (1986), discussed *supra* notes 34-35 & text.
[139] *Compare* Dow Chemical Co. v. United States, 476 U.S. 227, 238, 106 S.Ct. 1819, 1827 (1986) (use of sophisticated but publicly available (albeit very expensive) mapping camera did not constitute a search); Texas v. Brown, 460 U.S. 730, 739-740, 103 S.Ct. 1535, 1542 (1983) (use of flashlight did not constitute a search) *with* Kyllo, 533 U.S. at 40, 121 S.Ct. at 2046 (use of a thermal-imaging scanning device not in general public use constitutes a search).
[140] *See supra* notes 101-111 & text (discussing alternative view of *Katz* reasonable-expectation-of-privacy test).

warrant presumption should automatically apply. Some forms of surveillance may be so invasive that a presumptive warrant requirement would be appropriate almost without regard for the need for such surveillance. The government's collection and storage of digital metadata might be a good candidate for a presumptive warrant requirement, given the government's ever-growing technological capacity not only to collect, store and retrieve such data but to analyze those data in a way that permits increasingly accurate identification and real-time tracking of particular individuals, including prediction of their future movements.[141] In contrast, it may be that other, less-invasive technological surveillance for which there is demonstrated need which a warrant requirement might impede would not require a warrant to satisfy the Fourth Amendment's reasonableness requirement.

Consider a thermal scan of a house like that employed in *Kyllo*, which at bottom was no more than technologically enhanced visual surveillance. All that the scan revealed about Kyllo's house was the relative temperatures of various parts of its roof, which in turn suggested that certain interior spaces in the house were hotter than others. Even assuming that this information would have been unavailable unless agents entered the house, as a matter of common sense this does not justify treating these two searches – forcible entry versus an infrared roof scan – the same, requiring a warrant for each. Putting aside the trauma of a forcible entry and focusing just on privacy interests, a scan reveals heat emanating from various parts of the house whereas physically entering the house and roaming from room to room to determine the temperature of each necessarily reveals both contents and activities in the house. To be sure, Justice Scalia is correct in pointing out that the heat rising through the roof permits inferences about the activities within – perhaps including the time at which the "lady of the house takes her daily sauna and bath"[142] – but that does not justify equating the intrusiveness of a thermal scan with a full-blown search of the house.

Of course, the intrusiveness of a search is only half the story. The reasonableness balance includes the law-enforcement interest served by the search, including the need for the search in advancing that interest. Thermal scans such as those employed in *Kyllo* are used to detect patterns of heat emanation consistent with indoor marijuana cultivation, a relatively serious felony in most jurisdictions. While there certainly are other means of detecting evidence of this illegal activity, this investigative technique, narrowly tailored to its purpose, permits law enforcement officers quickly and efficiently to confirm or dispel suspicions of such illegality and is thus a useful law-enforcement technique for which there would appear to be no ready substitute.

---

[141] *See* James Risen & Eric Lichtblau, *How the U.S. uses Technology to Mine More Data More Quickly*, N.Y. Times, June 9, 2013, at 11 (describing a new technology, trilaterization, that "allows tracking of an individual's location, moment to moment. The data, obtained from cellphone towers, can track the altitude of a person, down to the specific floor in a building. There is even soft-ware that exploits the cellphone data seeking to predict a person's most likely route.").

[142] Kyllo, 533 U.S. at 38, 121 S.Ct. at 2045.

What would be the costs and benefits of requiring a search warrant in this context? As noted above, one potential benefit of a warrant is limiting the search's scope to the particular areas and particular items to be seized authorized by the magistrate based on the probable cause demonstrated in the warrant application. That limitation can be quite important in cabining officers' discretion if they enter and search a house, but a thermal scan is by nature limited in scope, and so the warrant would do little in this regard.[143] Presumably, a warrant would permit scanning the roof for infrared radiation, which is all that the scanner does. To be sure, a warrant would limit the discretion of the officers concerning what roof could be scanned and when that scan could be performed, but requiring officers to have individualized suspicion of marijuana cultivation as a predicate to a roof scan would provide a similar, though concededly less protective, limitation concerning which roof could be searched. Further, given the non-disruptive character of a roof scan – the occupants of the house would likely be unaware of its occurrence – the timing of the search would seem less important than the timing of a physical search of the house to determine the temperature of the house's various rooms, and there would seem to be no need to inform its occupants of the authority for a search of which they are unaware.

Of course, the main benefit of a warrant lies in the level of suspicion required to justify a search, probable cause, and the imposition of a neutral magistrate as the arbiter of probable cause, thus providing for a determination that the search is justified before it occurs and for a record of the basis for that determination that permits subsequent review. But this assumes that probable cause is the appropriate level of certainty required to justify this search. It may be, but the cost of requiring probable cause – and with it a warrant – to justify a roof scan is to eliminate it as an investigative tool. If the officers have probable cause to believe that there is marijuana cultivation within a building, they would not need a thermal scan to confirm that fact. Rather, they could secure a warrant authorizing a physical search of the premises for the marijuana. A warrant requirement in this context does not simply ensure that it is the neutral magistrate rather than the officer who determines that the search is justified; it ensures that no such search will occur. Given the interest balance involved, the cost of the extra protection provided by a warrant requirement may be too high. If that is so, it would not mean that thermal scans should be considered presumptively reasonable; it would only mean that the warrant presumption would be inapt for such surveillance.

Other forms of surveillance seem similarly, or almost certainly, inapt candidates for a warrant presumption. At one extreme would be naked-eye surveillance by a beat cop standing in a public place. The intrusiveness side of the reasonableness balance is far less weighty than those searches at the core of Fourth Amendment values, and the law-enforcement need for such traditional surveillance seems beyond question. And, even more than is so with thermal scans, it

[143] *Cf*. King, 569 U.S. at --, -- S.Ct. at --, Slip Op. No. 12-207 at 9 (Kennedy, J., for the Court) ("The need for a warrant is perhaps least when the search involves no discretion that could properly be limited by the 'interpo[lation of] a neutral magistrate between the citizen and the law enforcement officer") (citation omitted).

is difficult to see what function a warrant would serve. The observations of the cop on the beat, while searches, would seem to be presumptively reasonable, requiring no particularized justification to make them so. This presumptive reasonableness would be consistent with historical treatment of naked-eye observation, i.e., it is per se permissible, but the normative justification for this presumption would be that, while a search, the public need for such unfettered investigative observation outweighs any individual interest in avoiding it or in subjecting it to further constitutional oversight.

The same might not be so for surveillance more intrusive than the observations of a cop on the beat, whether or not the surveillance employs technology that is commonly available. Consider GPS surveillance conducted by monitoring tracking devices that were either factory- or owner-installed, that is, GPS surveillance that does not involve a trespass to chattels and is thus not covered by *Jones*. On the one hand, as the government argued in *Jones*,[144] this surveillance does no more than monitor and catalog the public whereabouts of the person who possesses a particular device, something that a properly positioned law enforcement officer (or team of officers) could theoretically observe. If such public observations by police are presumptively reasonable, the sum of those presumptively reasonable searches – more efficiently executed and accurately recorded by technology – is also presumptively reasonable. On the other hand, as Jones argued,[145] the matrix of precise information that four-week around-the-clock GPS surveillance yields is very intrusive, going well beyond public travel, revealing a great deal about the private life of the person who is subjected to the surveillance. This mode of surveillance is more intrusive than a beat cop's observations, or even a thermal scan of a house, but it is not clear that it matches the intrusiveness of searches that justify a warrant presumption.

Turning to the government side of the balance, the public-safety need for such surveillance, GPS tracking has potential application in a broad range of law-enforcement activities, ranging, for example, from tracking suspected drug dealers to tracking suspected terrorists plotting to use a weapon of mass destruction, one of Justice Alito's "extraordinary offenses."[146] Depending on the use to which it is put, there could be substantial law-enforcement need for such surveillance in circumstances that a warrant requirement might thwart, perhaps because of the probable-cause requirement or because of difficulties in readily securing a warrant.

Maybe, on balance, a warrant presumption would over-protect individual interests and under-value legitimate governmental interests in long-term GPS surveillance. Maybe a more reasonable accommodation of those competing interests would be to require a reasonable suspicion to justify such searches. Maybe the tracking of cars is sufficiently public that neither a warrant nor individualized suspicion is necessary. Maybe the most pressing concern is that the information thus gathered, stored and cataloged could be misused, a concern that might be

[144] *See* Brief for Petitioner at 17-33, United States v. Jones, 565 U.S. --, 132 S.Ct. 945 (2012) (No. 10-1259).
[145] *See* Brief for Respondent at 24-30, United States v. Jones, 565 U.S. --, 132 S.Ct. 945 (2012) (No. 10-1259).
[146] Jones, 565 U.S. at --, 132 S.Ct. at 964.

addressed by requiring police regulations governing its retrieval and use, which regulations could be reviewed by a court utilizing particular criteria to ensure that the regulations and their enforcement are adequate to protect against abuses of discretion.[147] But maybe the warrant presumption is the appropriate measure of Fourth Amendment reasonableness, relying on exceptions to the warrant requirement to suit particular applications for which a warrant is not suited (like Justice Alito's "extraordinary offenses"), much as is so with the warrant requirement currently in place.

However any of these examples of interest balancing might play out, the point is that once Fourth Amendment coverage is broadened to include all means of gathering information, the presumption of a warrant should not reflexively be the starting point in deciding whether or not a particular mode of search is reasonable. For traditional, physically invasive searches of houses or their analogs, the warrant presumption and its various exceptions are likely appropriate and thus would likely remain unchanged. So, too, highly invasive technological surveillance such as the National Security Agency's reported collection and analysis of metadata might require a warrant. However, for less-intrusive modes of search, it may be that the particular balance of interests suggests utilizing reasonable suspicion rather than probable cause to justify the search. Alternatively, particularly where the Fourth Amendment concern is as much for the potential abuse of official discretion as for the justification of the search, the interest balance may suggest an altogether different approach to defining reasonableness, perhaps one employing police rulemaking "created and maintained in working order [] by the stimulation and oversight of the courts enforcing constitutional law," as suggested by Prof. Amsterdam over 50 years ago.[148]

Conclusion

This suggested departure from the warrant presumption is one steeped in caution. I am mindful of the potential pitfalls once one departs from the warrant presumption, with its familiar, built-in requirement of probable cause as a measure of Fourth Amendment reasonableness. Defining Fourth Amendment protection by interest balancing is dangerous business. One need look no further than Justice Douglas's warning in *Terry* that without the "ring of certainty" provided by the deeply rooted requirement of probable cause, "powerful hydraulic pressures" grounded in apparent necessity will "bear heavily on the Court to water down constitutional guarantees and give the police the upper hand."[149] Whether Justice Douglas was correct in his prediction of loosened guarantees in stop and frisks,[150] it is surely true that the standard bearers

[147] *See* Camara v. Municipal Ct. of City and County of San Francisco, 387 U.S. 523, 532-533, 87 S.Ct. 1727, 1732-1733 (1967).
[148] *See* Anthony Amsterdam, *Perspectives on the Fourth Amendment*, 58 Minn. L. Rev. 349, 380 (1958).
[149] Terry v. Ohio, 392 U.S. 1, 37-39, 88 S.Ct. 1868, 1888-1889 (1968) (Douglas, J., dissenting).
[150] Statistics, at least, tell a story of widespread and apparently disproportionate stops and frisks of African-Americans and Hispanics in New York City. According to data that the Center for Constitutional Rights obtained from the city, of the 1.2 million persons that NYC police officers stopped in the past two years, 84% were either African-American or Hispanic, even though these two racial cohorts combine to make up only 52% of the City's

for individual rights are, for the most part, criminals who seem unworthy beneficiaries of limitations on governmental law-enforcement efforts. And, it is equally true that the government side of the balance is easy to over-value, particularly in an age of seemingly ubiquitous terrorist plots (punctuated by reported close calls and infrequent but tragic attacks), while the privacy-liberty side of the balance may seem an extravagance, particularly to those who cannot picture themselves subject to such investigative attention. Finally, any such interest balancing cannot be ad hoc. It must yield rules that are sufficiently clear to permit those who are bound to follow them – law-enforcement officials, lawyers and judges – to know what they mean and to consistently apply them.

That said, if we are to face up to the challenges that advancing technology poses to Fourth Amendment protection, it is essential that we do so in transparent terms. This means, as I have argued, that we recognize all information gathering by the government for what it is – a search – which would permit assessing the reasonableness of all modes of surveillance. That assessment requires, and will require, a careful and sophisticated balancing of interests, a balancing that a presumptive warrant requirement would hamstring if not foreclose. If we insist on applying this presumption beyond the searches for which it is the apt measure of Fourth Amendment reasonableness, the result will be distortions of Fourth Amendment doctrine, like *Katz*'s pretense that certain searches are not "searches," in a clumsy and indirect effort to correct the reasonableness balance.[151] Given the stakes, we cannot afford to trade one distortion for another.

---

population. *See* Bill Weir & Nick Capote, *NYPD's Controversial Stop-and-Frisk Policy: Racial Profiling or 'Proactive Policing'?*, ABC News Nightline, May 1, 2013 (available at http://abcnews.go.com/US/nypds-stop-and-frisk-policy-racial-profiling-proactitve/story?id=19084229). Statistics, of course, are contextual, and NYPD Commissioner Raymond Kelly defends the stop-and-frisk policy, arguing that, because almost three-quarters of the persons described to the police as perpetrators of violent crimes were described as being African-Americans, if anything African-Americans were being, in his words, "under stopped." *Id*. Whoever has the better of this statistical argument, most African-Americans who have been repeatedly stopped and frisked in New York do not feel "under stopped." *Id*. (17-year-old Brooklyn man describing his fear during the seven stops-and-frisks to which he says he has been subjected in his neighborhood). They likely would agree with Justice Douglas that their constitutional guarantees have been "watered down." And maybe then some.

[151] A good example of this phenomenon is *Maryland v. King*, 569 U.S. --, -- S.Ct. --, Slip Op. No. 12-207 (2013), in which the Court upheld a program of warrantless DNA testing of felony arrestees. There was no doubt but that the taking of the cells by cheek swab and subsequent DNA testing of those cells was a search. The question was, did that search require a warrant? Plainly mindful of the presumption that law-enforcement searches for evidence must be supported by a warrant, the Court went to great length to characterize the testing program as a means of identifying arrestees, Slip Op. at 10-13, 18-23 (Kennedy, J., for the Court), an administrative rather than a law-enforcement need. However, in his dissent Justice Scalia exposed the implausibility of that claim, pointing to record evidence that both on its face and in its operation the testing program was designed to solve unsolved crimes, a pure law-enforcement need. *See* Slip Op. No. 12-207 at 5-17 (Scalia, J., dissenting). The Court's conclusion that the testing program represented a "minor intrusion" on the defendant's privacy expectations that was outweighed by "significant state interests" and thus that the search was reasonable, Slip Op. No. 12-207 at 28, is at least a defensible balancing of the interests involved, but its strained insistence that the state's interests were administrative and not law-enforcement – all to avoid the warrant presumption – undercuts both the analytic force of the opinion and the credibility of the Court as a principled decision maker.