SHOUTING DOWN THE WELL: HUMAN OBSERVATION AS A NECESSARY CONDITION OF PRIVACY BREACH, AND WHY WARRANTS SHOULD ATTACH TO DATA ACCESS, NOT DATA GATHERING

*HAROLD LAIDLAW**

* J.D. 2014, N.Y.U. School of Law. Thanks to Professors Barry Friedman and Samuel Rascoff of the N.Y.U. School of Law for feedback and suggestions on this Note, and to the N.Y.U. Annual Survey of American Law for their patience and invaluable input during the publication process.

INTRODUCTION

On April 15, 2013, at 2:49 p.m., a pair of pressure cookers packed with black powder and shrapnel exploded at the Boston Marathon, killing three and wounding or maiming 264.[1] It was the worst act of terrorism on United States soil since September 11, 2001, and it took place amidst the most prestigious annual running event in the country, sowing mass chaos in a public space full of thousands of spectators.[2]

1. Criminal Complaint at 3, United States v. Tsarnaev, 951 F. Supp. 2d 209 (D. Mass. 2013) (No. 13-2106-MBB), 2013 WL 1715437; Deborah Kotz, *Injury Toll from Marathon Bombs Reduced to 264*, BOSTON GLOBE (Apr. 24, 2013), http://www.bostonglobe.com/lifestyle/health-wellness/2013/04/23/number-injured-marathon-bombing-revised-downward/NRpaz5mmvGquP7KMA6XsIK/story.html.

2. Josh Levs & Monte Plott, *Boy, 8, One of 3 Killed in Bombings at Boston Marathon; Scores Wounded*, CNN (Apr. 18, 2013, 10:25 AM), http://www.cnn.com/2013/04/15/us/boston-marathon-explosions.

Within three days the FBI had released images of the suspects.[3]

In the wake of the respective capture and killing of perpetrators Dzhokar and Tamerlan Tsarnaev, Boston Police Commissioner Edward Davis stated that he believed the release of the images to have been a "turning point" in the investigation.[4] Following the release of the images the brothers' actions became increasingly aggressive and public, culminating in the brutal murder of an MIT police officer, a carjacking, a chaotic police chase, and the lockdown of a significant section of the Boston area.[5] This chase eventually resulted in the death of one bomber and the apprehension of the other.[6]

There had been little official suspicion of the brothers Tsarnaev,[7] who apparently acted essentially alone.[8] Given the enormous throng surrounding the marathon, the chances for witness identification of the bombers were slim.[9] In the immediate aftermath of the carnage, the fact that acts of terrorism were now a realized risk at public gatherings was disturbing to acknowledge; perhaps even more disturbing, however, was the prospect that such acts could be committed by anonymous villains with impunity.

Ultimately the FBI was able to identify several images of the bombers not because of a star witness but through painstaking review of video footage of the scene from both public and private

3. Katharine Q. Seelye, et al., *F.B.I. Posts Images of Pair Suspected in Boston Attack*, N.Y. TIMES, Apr. 19, 2013, at A1.

4. Milton J. Valencia, *Davis Calls Releasing Photos a "Turning Point,"* BOSTON GLOBE (Apr. 21, 2013), http://www.bostonglobe.com/2013/04/20/boston-police-commissioner-edward-davis-says-releasing-photos-was-turning-point-boston-marathon-bomb-probe/cMV6bScwrbJZn90liq4YWP/story.html.

5. *See* Michael S. Schmidt & Eric Schmitt, *Manhunt's Turning Point Came in the Decision to Release Suspects' Images*, N.Y. TIMES, Apr. 21, 2013, at A21.

6. *See id.*

7. In 2011 the FBI had investigated and interviewed Tamerlan Tsarnaev in response to a request from Russian authorities alleging his involvement with radical Islamists. Eric Schmitt & Michael S. Schmidt, *Investigators Dig for Roots of Bomb Suspects' Radicalization*, N.Y. TIMES, Apr. 22, 2013, at A1. The results of the investigation, however, had exonerated him of suspicion. *Id.*

8. *See* Bryan Bender, *Boston Officials Say Tsarnaev Brothers Acted Alone*, BOSTON GLOBE (Apr. 21, 2013), http://www.bostonglobe.com/metro/2013/04/21/boston-officials-say-tsarnaev-brothers-planned-for-more-violence-but-were-acting-alone/9FthniLFxGARqmKVimATrJ/story.html.

9. *See* Schmitt & Schmidt, *supra* note 7. Notably, however, Jeff Bauman, who lost both legs in the bombing, recalled several salient details about Dhozkhar Tsarnaev upon waking up in the hospital. Asjylyn Loder & Esmé E. Deprez, *Boston Bomb Victim in Photo Helped Identify Suspects*, BLOOMBERG (Apr. 19, 2013), http://www.bloomberg.com/news/2013-04-19/boston-bombing-victim-in-iconic-photo-helped-identify-attackers.html.

sources.[10] It was a powerful demonstration that the availability of abundant data—data otherwise subject to a life of essentially mundane repose—could prove essential to a crucial national security investigation.

Nevertheless the nature of the investigation also made starkly apparent the degree to which recording of public spaces had become routine,[11] and the degree to which law enforcement could access such information from both private and public sources.[12]

As law enforcement continues to seek ever-expanding surveillance capabilities,[13] the dissolution of effective anonymity in public

10. *See* Press Release, FBI, Remarks of Special Agent in Charge Richard DesLauriers at Press Conference on Bombing Investigation (Apr. 18, 2013), *available at* http://www.fbi.gov/boston/press-releases/2013/remarks-of-special-agent-in-charge-richard-deslauriers-at-press-conference-on-bombing-investigation-1 (discussing release of photographs of Boston Bombing suspects and requesting public help in identifying them); David Montgomery et al., *FBI Releases Images of Two Suspects in Boston Marathon Bombings*, WASH. POST (Apr. 18, 2013), http://www.washingtonpost.com/world/national-security/investigators-focus-on-video-of-two-men-at-scene-of-boston-marathon-bombings/2013/04/18/6dadfcfa-a833-11e2-8302-3c7e0ea97057_story.html ("Napolitano spoke a day after the daunting task of sifting through thousands of images of the Boston Marathon bombing site in search of a culprit suddenly telescoped to a video from a Lord & Taylor security camera."). *See generally* Taryn Luna, *FBI Sifting for Clues in Mountains of Evidence*, BOSTON GLOBE (Apr. 17, 2013), http://www.bostonglobe.com/business/2013/04/16/software-tools-offer-limited-help-fbi-agents-analyzing-marathon-video/mXM8fYyBDY8B05iJj1UaLN/story.html.

11. *See* Luna, *supra* note 10 (quoting Grant Fredericks, leader of the investigation into the Vancouver Riots in the wake of the 2011 Stanley Cup, for the proposition that the total amount of private and public recording at the Boston Marathon was such that "they probably have every inch of that event covered for every second of that day").

12. *See id.* Another recent example of law enforcement's use of municipal surveillance infrastructure was the investigation of the 2012 Empire State Building shooting, in which nine bystanders were injured by the discharge of sixteen bullets fired by police at alleged gunman Jeffrey Johnson. James Barron, *Gunman Dies After Killing at Empire State Building*, N.Y. TIMES, Aug. 25, 2012, at A1. At least one injured bystander eventually sued the city, alleging that the NYPD officers who injured her had negligently confronted the gunman. J. David Goodman, *Bystander Shot near Empire State Building Sues Police*, N.Y. TIMES, Jan. 23, 2013, at A18. The bystander's complaint referred to the availability of a video showing the conduct of the officers, who shot repeatedly at Johnson when he brandished a pistol after being confronted. *Id.*; *see also* Barron, *supra* (containing inset video showing events of shooting).

13. For instance, law enforcement across the county is increasingly integrating the use of unmanned surveillance drones into their arsenals, often provoking a harsh legislative response and outrage from civil libertarians. *See, e.g.*, *Domestic Drones*, ACLU BLOG OF RIGHTS, http://www.aclu.org/blog/tag/domestic-drones (last visited Mar. 29, 2015); Martin Kaste, *As Police Drones Take Off, Washington State Pushes Back*, NPR (Feb. 22, 2013), http://www.npr.org/2013/02/22/172696814/

space—in particular, anonymity from the eyes of government—has not escaped the notice of commentators.[14] Civil libertarians have voiced concerns about the capacity of ubiquitous surveillance infrastructure to alter the traditional balance of power between the government as observer and the citizenry as observed,[15] codified in the Fourth Amendment's guarantee of freedom from unreasonable searches and seizures.[16] In particular, even as it facilitates national security investigations, ubiquitous surveillance threatens to compromise public anonymity in the form of "the right to be let alone."[17]

This Note aims to develop a set of constitutional rules for the ubiquitous surveillance of public space, and for the collation of data gathered therefrom—mining, sorting, and sifting through such data—that conforms to existing precedent while recognizing that recent Supreme Court cases, most notably *United States v. Jones*[18] and *Riley v. California*,[19] have signaled a willingness by the Court to adopt a new jurisprudence sensitive to the capacity of technological advance to compromise privacy.

Parts I and II first argue that although the Supreme Court's traditional Fourth Amendment jurisprudence has focused on protection of the individual's "reasonable expectation of privacy,"[20] there has been very little effort by courts to define precisely what privacy is. In particular, the lack of focus on privacy as a concept distinct from social convention has inhibited the formulation of a legal definition of privacy *breach*. The advancement of technology,

---

as-police-drones-take-off-washington-state-pushes-back (stating that Seattle, in 2013, became one of the first cities in the United States to buy unmanned drones for use by the police department); Jason Koebler, *Law Enforcement Blindsided by Public "Panic" Over Drone Privacy*, U.S. NEWS (Mar. 21, 2013), http://www.usnews.com/news/articles/2013/03/21/law-enforcement-blindsided-by-public-panic-over-drone-privacy. Likewise many police departments, including New York City's, are running pilot programs in which police-civilian interactions are recorded by cameras worn by law enforcement officers. J. David Goodman, *City Police Officers Will Start Using Body Cameras in a Pilot Program*, N.Y. TIMES, Sept. 5, 2014, at A19.

14. *See, e.g.*, Goodman, *supra* note 12.

15. *See, e.g.*, *Rein in the Surveillance State*, ACLU, https://www.aclu.org/rein-surveillance-state (last visited Feb. 16, 2015, 11:52 AM) ("Our Constitution and democratic system demand that government be transparent and accountable to the people, not the other way around. History has shown that powerful secret surveillance tools will almost certainly be abused for political ends.").

16. *See* U.S. CONST. amend. IV.

17. Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

18. 132 S. Ct. 945 (2012).

19. 134 S. Ct. 2473 (2014).

20. *See, e.g.*, Katz v. United States, 389 U.S. 347, 360–61 (1967); *see also infra* Part I.

however, increasingly brings this question to the fore as passive data gathering becomes conceptually distinct from active data analysis by a human law enforcement officer. Because, as this Note argues, a privacy breach cannot occur without this latter, human-initiated analysis stage, there are sound constitutional and normative reasons to place restrictions only on the access and use of data rather than on its gathering and availability.

Part III then develops some of the implications of a constitutional regime that attaches the Fourth Amendment warrant requirement to data access. The need for a technology-sensitive Fourth Amendment jurisprudence only arises when the background presumptions underlying previous Fourth Amendment cases cease to hold[21]—that is, when technology amplifies the information-gathering capacity of law enforcement far beyond what individual officers could accomplish in decades past. Therefore novel restrictions on data access should only attach when government agents interact with novel surveillance infrastructure. Such restrictions should not apply to the access of essentially administrative data available to the government as a matter of course. This Note also argues that as a matter of pragmatic necessity, the data needed to identify individuals cannot be a subject of ex ante warrant protection.

Lastly, Parts IV and V discuss the normative dimensions of a use-restriction Fourth Amendment paradigm. In addition to preserving reliance interests in surveillance infrastructure, a rule that the warrant requirement attaches at the point of human access to data is desirable both due to its clear conduct guidance for law enforcement and for its straightforward application by judges adjudicating Fourth Amendment claims. In contrast, imposing Fourth Amendment restrictions at the point of data gathering risks creating constitutional inconsistencies necessitating logical contortions at odds with the trajectory of important precedents. Allowing unfettered data gathering inevitably poses the risk of government abuses against which the Fourth Amendment is intended to guard. However, the same surveillance infrastructure used to gather information about everyday citizens can also be used to mitigate the risk of such abuses by providing auditable records of government activity and ensuring that government agents are accountable for their use of data. Accordingly this Note argues that ubiquitous surveillance is desirable as a means to ensure the availability of objective evidentiary records, but that technologically sensitive Fourth Amendment

21. *See infra* Part II.C.

principles suggest restrictions on access to such records. The United States ought to embrace the Panopticon[22] but take care to watch the watchers.[23]

I.
BACKGROUND

A. The Current Protections—Or Lack Thereof— Surrounding Collation of Public Data: Katz *to* Knotts

The ever-increasing availability of data as a result of encroaching technology, and the need for a judicial response to its implications, has hardly escaped the notice of the Supreme Court. As early as 1971 Justice Harlan adverted to the distinction between the limited capacity of human recall and the fallibility of witness narratives versus the remorseless accuracy of objective recordings:

> The argument . . . that it is irrelevant whether secrets are revealed by the mere tattletale or the transistor, ignores the differences occasioned by third-party monitoring and recording which insures full and accurate disclosure of all that is said, free of the possibility of error and oversight that inheres in human reporting.[24]

It was in fact technology's ever-advancing capacity to compromise previously sacrosanct data that first led the Court to expand beyond its previous, exclusively trespass-oriented understanding of

22. The term refers to Jeremy Bentham's classic idea for a penitentiary structure in which inmates would be subject to potential observation at all times, although they would remain unaware of precisely when they were being observed. *See generally* JEREMY BENTHAM, THE PANOPTICON WRITINGS 29–95 (Miran Bozovic ed., 1995).

23. The common Latin formulation of this phrase is the well-known expression *quis custodiet ipsos custodes?*

24. United States v. White, 401 U.S. 745, 787 (1971) (Harlan, J., dissenting). Ironically Justice Harlan's dissent was intended to *criticize* the use of objective recordation of data for evidentiary purposes, a point of view that seems difficult to square with the idea that the finder of fact should be presented with "full and accurate disclosure" as opposed to narratives filled with "error and oversight." *See id.* at 787–90. However, Justice Harlan's chief concern in *White* was arguably the effect of ubiquitous recordation on First Amendment free discourse rather than Fourth Amendment privacy—a concern recently echoed by Professor Katherine Strandburg with respect to another First Amendment expressive freedom, that of assembly. *See* Katherine J. Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. REV. 741, 747 (2008) (arguing that relational surveillance—a form of surveillance that allows the government to study connections between individuals—may "pose[ ] serious risks . . . to the First Amendment rights of freedom of association and assembly").

the Fourth Amendment in *Katz v. United States*.[25] Katz, a wildly successful gambler, found himself facing criminal prosecution after law enforcement placed an eavesdropping device on a public telephone he used to place bets with bookies in remote cities.[26] Reversing precedent the Supreme Court held that the lack of *physical intrusion* (that is, trespass) into any protected area was not dispositive.[27] Writing a concurrence adopted by later Court majorities,[28] Justice Harlan articulated the following test: in evaluating whether a law enforcement action constituted a search and required a warrant, courts were to determine (1) whether the person subject to the search had exhibited a subjective expectation of privacy in the object of the search, and (2) whether society was prepared to recognize such an interest as reasonable.[29] *Katz* and its progeny have formed the backbone of Fourth Amendment analysis ever since.[30]

B. "Knowingly Exposed to the Public": Exposure in Principle Means No Protection in Practice

A corollary to the second prong of the *Katz* inquiry—whether society at large is prepared to recognize a privacy interest as reasonable—is that "what a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[31] Thus information that can be *observed* by the public using only human sensory perception is generally not protected under *Katz*.

---

25. 389 U.S. 347 (1967).

26. David A. Sklansky, Katz v. United States*: The Limits of Aphorism*, *in* CRIMINAL PROCEDURE STORIES 224, 224 (Carol S. Steiker ed., 2006); Carol S. Steiker, *Brandeis in* Olmstead*: "Our Government Is the Potent, the Omnipresent Teacher*," 79 MISS. L.J. 149, 160 (2009).

27. *Katz*, 389 U.S. at 353. The Court has recently held, however, that in cases involving an unambiguous trespass the trespass itself constitutes a Fourth Amendment violation if performed without a warrant. United States v. Jones, 132 S. Ct. 945, 952 (2012) ("But as we have discussed, the *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test."); *see also infra* note 34; *cf. infra* note 34.

28. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 32–35 (2001) (adopting the Harlan test); California v. Ciraolo, 476 U.S. 207, 211 (1986) (describing the two-part *Katz* test as "[t]he touchstone of Fourth Amendment analysis"); Smith v. Maryland, 442 U.S. 735, 740 (1979) (endorsing the "reasonable expectations" test as correct Fourth Amendment gravamen and collecting cases); *see also Jones*, 132 S. Ct. at 950 ("Our later cases have applied the analysis of Justice Harlan's concurrence in [*Katz*], which said that a violation occurs when government officers violate a person's "reasonable expectation of privacy.").

29. *Katz*, 389 U.S. at 360–61 (Harlan, J., concurring).

30. *See* cases cited *supra* note 28.

31. *Katz*, 389 U.S. at 351 (majority opinion), 361 (Harlan, J., concurring).

Cases in the wake of *Katz* clarified that as long as information *could* be passively observed by the public, it would not be subject to the Fourth Amendment warrant requirement.[32] In particular the empirical likelihood of *actual* observation by the public was generally held not to bear on whether police action constituted a search.[33] Rather the police had at least as much freedom to snoop in their capacity as law enforcement officers as they had in their capacity as private citizens,[34] subject to certain restrictions on the

32. *See generally* cases cited *infra* notes 33 and 42 and accompanying text.

33. *See* California v. Greenwood, 486 U.S. 35, 41 (1988) (emphasis added) (upholding the warrantless police search of opaque trash bags because "the police cannot reasonably be expected to avert their eyes from evidence of criminal activity that *could have been observed by any member of the public*"); *Ciraolo*, 476 U.S. at 211, 213–14 (emphasis added) (upholding a warrantless aerial search for marijuana plants from aircraft at 1000 feet despite a surrounding fence exhibiting subjective intention of privacy on the theory that "[a]ny member of the public flying in this airspace who glanced down *could have* seen everything that these officers observed"); *cf.* Florida v. Riley, 488 U.S. 445 (1989) (affirming validity of warrantless viewing of marijuana plants of defendant from helicopter at 400 feet through holes in greenhouse roof in fenced-in yard). Although the plurality opinion of *Riley* found little to distinguish it from *Ciraolo*, Justice O'Connor's concurrence in judgment, which was necessary to the outcome of the case, argued that the empirical likelihood of helicopters hovering 400 feet over a private residence should constitute a factor in determining the reasonableness of an expectation of privacy. *Riley*, 488 U.S. at 454 (O'Connor, J., concurring) ("[W]e must ask whether the helicopter was in the public airways at an altitude at which members of the public travel with sufficient regularity that Riley's expectation of privacy from aerial observation was not one that society is prepared to recognize as 'reasonable.'"). Somewhat counterintuitively, however, Justice O'Connor concluded that the defendant had not met the burden of showing that helicopters flying over single-family homes at 400 feet was not an occurrence of "sufficient[ ] regularity" to warrant suppression of the evidence, "because there is reason to believe that there is considerable public use of airspace at altitudes of 400 feet and above, and because Riley introduced no evidence to the contrary before the Florida courts." *Id.* at 455.

34. In at least some important respects the police in fact have *more* power to gather evidence without fear of suppression than they would in their capacity as private citizens. The "open-fields" doctrine, for instance, precludes suppression of evidence gained from a police trespass on private property unless law enforcement encroaches on the "curtilage of a home." United States v. Dunn, 480 U.S. 294, 304 (1987) (invoking *Oliver* and *Hester* in support of police looking through barn windows on suspect's property in wake of warrantless trespass); Oliver v. United States, 466 U.S. 170, 178 (1984) (affirming *Hester* and limiting the cognizable expectation of privacy to "the area immediately surrounding the home"); Hester v. United States, 265 U.S. 57, 59 (1924) ("[T]he special protection accorded by the Fourth Amendment to the people in their 'persons, houses, papers and effects,' is not extended to the open fields."). Likewise in *California v. Greenwood*, the Court rejected Greenwood's contention that California law's proscription on warrantless garbage searching was sufficient to provide a Fourth Amendment privacy guarantee. 486 U.S. at 43 ("We have never intimated, however, that whether or not a

use of technology "not in general public use" to view information emanating from the home.[35]

United State v. Knotts stands for the proposition that an action is considered "exposed to the public" not by virtue of whether it is *in fact* viewed by onlookers, but by virtue of the action's nature and place of occurrence—the public character of an action is an intrinsic property rather than a function of who does or does not actually observe it.[36] In *Knotts* law enforcement had placed an electronic monitoring device known as a "beeper" into a drum of chloroform bound for a drug lab.[37] Police initially followed defendant Darryl Petschen's car containing the drum but lost sight of him after he began taking evasive maneuvers.[38] However, law enforcement authorities nevertheless managed to relocate the chloroform drum at a rural cabin (home to the aforementioned drug lab) after tracking the beeper signal from a helicopter.[39] Rejecting codefendant

search is reasonable within the meaning of the Fourth Amendment depends on the law of the particular State in which the search occurs.").

35. Kyllo v. United States, 533 U.S. 27, 34 (2001) (holding that warrantless use of a thermal imager to view heat passively emanating from a home infringed the Fourth Amendment's special protection for people in their own homes).

36. United States v. Knotts, 460 U.S. 276, 281–82 (1983) (emphasis added) ("A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another. When [Defendant] traveled over the public streets he voluntarily conveyed to anyone who wanted to look the fact that he was traveling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property. . . . Visual surveillance from public places along Petschen's route or adjoining Knotts' premises *would have sufficed* to reveal all of these facts to the police. The fact that the officers in this case relied not only on visual surveillance, but also on the use of the beeper to signal the presence of Petschen's automobile to the police receiver, does not alter the situation."); *cf.* California v. Ciraolo, 476 U.S. 207, 212–13 (finding no Fourth Amendment violation under *Knotts*/*Katz* because "[a]ny member of the public flying in this airspace who glanced down could have seen everything that these officers observed."). In his dissent in *Ciraolo* Justice Powell interpreted *Knotts*, "Comings and goings on public streets are public matters, and the Constitution does not disable police from observing what every member of the public can see." *Ciraolo*, 476 U.S. at 224 (Powell, J., dissenting). Justice Powell also criticized the majority's extension of *Knotts* to aerial surveillance of a home because "[t]he activity in this case . . . took place within the private area immediately adjacent to a home. Yet the Court approves purposeful police surveillance of that activity and area similar to that approved in *Knotts* with respect to public activities and areas." *Id.*

37. *Knotts*, 460 U.S. at 278.

38. *Id.*

39. *Id.* at 278–79. The officers relied on the beeper information, along with information obtained from visual surveillance to secure a warrant authorizing the search of the cabin. *Id.* at 279.

Knotts' contention that the tracking of the beeper information constituted a search, the Supreme Court first stated that the *possibility* (albeit unlikely) that the police could have ascertained Petschen's whereabouts by piecing together other, cumulative knowledge—namely, the knowledge of potential passersby—precluded a cognizable privacy interest in his comings and goings:

> A person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another. When Petschen travelled over the public streets he voluntarily conveyed to anyone who wanted to look the fact that he was travelling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property.[40]

Addressing the specific contention that, but for the use of advanced technology, Petschen would have *in fact* eluded even determined efforts to track his location, the Court denied that the proliferation of information enabled by enhanced technology was a constitutionally cognizable issue—at least not yet:

> [S]cientific enhancement of this sort raises no constitutional issues which visual surveillance would not also raise. A police car following Petschen at a distance throughout his journey could have observed him leaving the public highway and arriving at the cabin owned by respondent, with the drum of chloroform still in the car.[41]

The implications of this language for ubiquitous search and data collation were clear: because privacy interests do not attach to activities that are *in principle* subject to observation by the public, law enforcement has essentially unlimited discretion to monitor such activities. By eliding the distinction between "nominally subject to observation" and "subject to observation within the range of means practically available to the public," the Court essentially gave its blessing to warrantless government surveillance of public space. This interpretation was followed in a number of later Supreme Court and Courts of Appeals cases.[42]

---

40. *Id.* at 281–82.

41. *Id.* at 285.

42. *E.g.*, California v. Ciraolo, 476 U.S. 207, 213 (1986) (citing *Knotts*, 450 U.S. at 282) ("[T]he mere fact that an individual has taken measures to restrict some views of his activities [does not] preclude an officer's observations from a public vantage point where he has a right to be and which renders the activities clearly visible."); United States v. Karo, 468 U.S. 705, 715, 721 (1984) (quoting *Knotts*, 460 U.S. at 281) (holding that no privacy interest in ether container's

C. "Twenty-Four Hour Surveillance": The Knotts *Dictum*

Ironically, however, *Knotts*—a Supreme Court opinion often cited for the proposition that activity knowingly exposed to the public is incompatible with the maintenance of a privacy interest—contains language implicitly disapproving of the unfettered surveillance of public space:

> Respondent . . . expresses the generalized view that the result of the holding sought by the government would be that "twenty-four hour surveillance of any citizen of this country will be possible, without judicial knowledge or supervision." . . . *[I]f such dragnet type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable.*[43]

In the context of the rest of the *Knotts* opinion, this statement appears to be a classic example of advisory dictum. At face value it suggests that a core holding of *Knotts*—that "scientific enhancement [of public-space surveillance] raises no constitutional issues which visual surveillance would not also raise"[44]—is correct only so long as it does not enable "twenty-four hour surveillance"[45]—in other words so long as it is not taken too far. The implication that the correctness of the *Knotts* rationale depends on its not being taken especially seriously—hardly consistent with the Court's desire to cabin lower courts' discretion—suggests that the language is more naturally read as having rhetorical rather than substantive character. In fact later in the very same paragraph the *Knotts* Court seemingly disclaimed the significance of the allusion to "twenty-four hour surveillance" by reiterating that the Supreme Court had

whereabouts under *Knotts* so long as it was on public byways, noting, "The information obtained in *Knotts* was 'voluntarily conveyed to anyone who wanted to look . . . .'"); United States v. Skinner, 690 F.3d 772, 777–78 (6th Cir. 2012) (holding that cellular phone location tracking for cross-country drug transport requires no warrant under *Knotts*); Autoworld Specialty Cars, Inc. v. United States, 815 F.2d 385, 388 (6th Cir. 1987) (holding that no warrant is required for search of privately owned business premises open to the public); United States v. Butts, 729 F.2d 1514, 1517 (5th Cir. 1984) (applying *Knotts* to movements of an aircraft in public airspace); United States v. Mankani, 738 F.2d 538, 544–45 (2d Cir. 1984) (finding that *Knotts* supports proposition that listening through crack in hotel room wall does not require a warrant because hotels are "transitory places" unlike homes).

43. *Knotts*, 460 U.S. at 283–84 (1983) (emphasis added) (citations omitted).

44. *Id.* at 285.

45. *Id.* at 283 (quotation marks omitted)

"never equated police efficiency with unconstitutionality, and we decline to do so now."[46]

Yet the Court's concession that, were police surveillance to become *too* pervasive, "different constitutional principles may be applicable"[47] is nevertheless an explicit acknowledgment that "police efficiency" *does* have implications for Fourth Amendment law. Although at first glance a seemingly innocuous rhetorical flourish, the *Knotts* dictum would later play a key role in the D.C. Circuit's opinion in *United States v. Maynard*, a case involving location tracking that, on certiorari, would become one of the most important Supreme Court surveillance opinions in recent history: *United States v. Jones*.[48]

D. Exploiting the Knotts *"Dictum":* Maynard *and the Cracks in the "Publicly Exposed" Façade*

Maynard was a narcotics conspiracy case.[49] The suspected heads of the operation, Antoine Jones and Lawrence Maynard, were meticulous about keeping their contact with the narcotics themselves to a minimum.[50] Seeking to gather evidence to link Jones and Maynard to the conspiracy, the D.C. police placed a GPS tracking device, about the size of a credit card, onto Jones's vehicle.[51] They did not, however, have a valid warrant.[52] Having tracked Jones' movements for four weeks and having correlated them with those of his coconspirators,[53] the government successfully charged and convicted Jones and Maynard.[54]

On appeal the defendants successfully sought the exclusion of the evidence gathered by means of the GPS device due to the absence of a warrant.[55] Disagreeing with recent Seventh, Eighth, and

46. *Id.* at 284.

47. *Id*.

48. 615 F.3d 544 (D.C. Cir. 2010), *aff'd in part sub nom.* United States v. Jones, 132 S. Ct. 945 (2012).

49. 615 F.3d at 548.

50. Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 321 (2012).

51. *Jones*, 132 S. Ct. at 957 n.1 (Alito, J., concurring).

52. In fact a warrant for the tracker had been obtained, but had expired prior to the tracker's attachment. *See Jones*, 132 S. Ct. at 948. The government nevertheless sought to establish that, under *Knotts*, the absence of a valid warrant was moot. *Maynard*, 615 F.3d at 566 n.*; *see also Jones*, 132 S. Ct. at 948 & n.1.

53. *Maynard*, 615 F.3d at 555.

54. *Id.* at 549.

55. *See Jones*, 132 S. Ct. at 949.

Ninth Circuit opinions on the same subject,[56] the D.C. Circuit held that the government's activities implicated the allusion in *Knotts* to "twenty-four hour surveillance":

> Most important for the present case, the Court specifically reserved the question whether a warrant would be required in a case involving "twenty-four hour surveillance," stating "if such dragnet-type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable."[57]

The future alluded to in *Knotts* was here, and despite a calendar year of 2010 it looked disturbingly like 1984.[58] The *Maynard* court accordingly found for defendant Jones and held that prolonged GPS tracking of a vehicle on a public street required the use of a warrant.[59]

The D.C. Circuit in *Maynard* specifically adverted to the dangers of *collated*[60] and *prolonged* information gathering:

> Two considerations persuade us the information the police discovered in this case—the totality of Jones's movements over the course of a month—was not exposed to the public: First,

56. *See Maynard*, 615 F.3d at 557–58 (declining to follow *United States v. Marquez*, 605 F.3d 604 (8th. Cir. 2010), and finding that defendant lacked standing to challenge GPS device tracking, but that even with standing *Knotts* controlled in such a way as to preclude the warrant requirement for GPS tracking); United States v. Pineda-Moreno, 591 F.3d 1212, 1216 (9th Cir. 2010), *vacated*, 132 S. Ct. 1533 (2012) (warrantless GPS tracking not a search under *Knotts*); United States v. Garcia, 474 F.3d 994 (7th Cir. 2007) (warrantless GPS tracking not a search under *Knotts*). The D.C. Circuit noted that all of the circuits to consider the issue had expressly reserved the *Knotts* question as to "mass" surveillance. *Maynard*, 615 F.3d at 558.

57. *Maynard*, 615 F.3d at 556 (quoting United States v. Knotts, 460 U.S. 276, 283–84 (1983)).

58. *See* GEORGE ORWELL, NINETEEN EIGHTY-FOUR (1949). This Note is far from alone in invoking the Orwellian dimensions of the current judicial scrutiny of technologically enabled ubiquitous surveillance. *See, e.g.*, *Pineda-Moreno*, 617 F.3d at 1121 (Kozinski, J., dissenting) ("1984 may have come a bit later than predicted, but it's here at last."). Judge Kozinski's passionate dissent of the Ninth Circuit's refusal to provide en banc rehearing in *Pineda-Moreno* is essentially a treatise on the perceived shortcomings of Fourth Amendment doctrine to adequately rein in ubiquitous government surveillance. *See id.* at 1123–27.

59. *Maynard*, 615 F.3d at 560, 568.

60. "Collating" data, as used in this Note, refers to the action of assembling and compiling disparate pieces of information to create a gestalt picture greater than the sum of its parts. The action is closely related to and largely synonymous with the mosaic theory of search advanced by commentators such as Orin Kerr. *See* Kerr, *supra* note 50.

> unlike one's movements during a single journey, the whole of one's movements over the course of a month is not actually exposed to the public because the likelihood anyone will observe all those movements is effectively nil. Second, the whole of one's movements is not exposed constructively even though each individual movement is exposed, because that whole reveals more—sometimes a great deal more—than does the sum of its parts.[61]

The Supreme Court had previously adverted to the privacy hazards of collated data when it invoked them to limit FOIA disclosures, but it had never applied any such rationale in the Fourth Amendment sphere.[62] The *Maynard* court accordingly adopted a uniquely expansive conception of Fourth Amendment protection, one that was sensitive to the capacity for collated information in sufficient quantity to compromise a background expectation of privacy that had hitherto been kept sacrosanct by *practical* constraints on knowledge and manpower rather than by formalistic search doctrine.[63]

On the one hand, *Maynard*'s expansive notion of search seemed invited by *Knott*'s reference to the development of expansive surveillance technologies: "if . . . dragnet type law enforcement practices . . . should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable."[64] In effect the *Knotts* dictum signaled to the *Maynard* court that the judiciary need not remain blind to the idea that information scarcity was increasingly ephemeral, yet also a background assumption of Fourth Amendment privacy jurisprudence.[65]

---

61. *Maynard*, 615 F.3d at 558.

62. *See* U.S. Dep't. of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 780 (1989) (justifying the withholding of an individual's compiled "rap sheet" of offenses despite the fact that all the information contained therein was technically part of the public domain); *see also Maynard*, 615 F.3d at 561 (invoking *Reporters Committee* for proposition that nominally public but nevertheless disparate bits of information have a greater capacity to compromise privacy as a collated gestalt than as simply uncollated pieces of information).

63. *Maynard*, 615 F.3d at 565 (noting that the D.C. Circuit had no occasion to review the significance of its holding for a visual search because "[f]or . . . practical reasons, and not by virtue of its sophistication or novelty, the advent of GPS technology has occasioned a heretofore unknown type of intrusion into an ordinarily and hitherto private enclave").

64. United States v. Knotts, 460 U.S. 276, 284 (1983).

65. *See, e.g.*, Klayman v. Obama, 957 F. Supp. 2d 1, 35–36, (D.D.C. 2013) (discussing constitutionality of NSA surveillance programs in the wake of the Edward Snowden disclosures and highlighting inadequacy of jurisprudence that failed to account for technological change). The *Klayman* court observed:

A jurisprudence hitherto characterized by a binary regime in which certain activities were or were not "searches" with attendant Fourth Amendment warrant requirements, and in which the police had essentially free reign to conduct observations that did not rise to the level of a "search,"[66] was increasingly insufficient to uphold any of the substantive values that privacy nominally represented.[67] In essence the system of binary procedural rules had been outmoded by the progress of technology, such that the exclusive focus on the conduct of the police had managed to undermine the substantive right at issue.

On the other hand, the line-drawing problems of a "prolonged surveillance" or "collated surveillance" test were readily apparent: How much information was too much? The overwhelming majority of *Katz*-related Supreme Court jurisprudence had been decided with respect to whether certain types of police conduct were searches in a categorical sense, rather than depending on the magnitude of the intrusion.[68] Ultimately the Supreme Court provided a resolution to the case at hand, while leaving many of the larger issues implicated unresolved.

E. Maynard *to* Jones*: The Return of Trespass, but a Majority of the Court Expresses a Willingness to Go Further*

The Supreme Court granted certiorari on *Maynard*, which by this point fell on one side of a circuit split between the D.C. Circuit on the one hand, and the Seventh, Eighth, and Ninth Circuits on the other.[69] The resulting case, *United States v. Jones*,[70] was ultimately

> Admittedly, what metadata is has not changed over time. As in *Smith*, the types of information at issue in this case are relatively limited: phone numbers dialed, date, time, and the like. But the ubiquity of phones has dramatically altered the quantity of information that is now available and, more importantly, what that information can tell the Government about people's lives.

Id. Klayman cites to *Maynard*'s "mosaic" approach approvingly. *Id.* at 36.

66. *See* Kerr, *supra* note 50, at 316 (emphasis added) ("[T]he basic structure of existing Fourth Amendment law . . . *starts with the threshold question of defining a search*, then turns to constitutional reasonableness, and concludes with Fourth Amendment remedies.").

67. *See supra* note 15 and accompanying text.

68. *See, e.g.*, Riley v. California, 134 S. Ct. 2473, 2491–92 (2014) (invoking the "general preference to provide clear guidance to law enforcement through categorical rules"); *see also supra* note 27.

69. *Compare* United States v. Maynard, 615 F.3d 544, 557–58 (D.C. Cir. 2010) (upholding a warrant requirement for GPS surveillance), *with* United States v. Marquez, 605 F.3d 604 (8th. Cir. 2010) (finding that defendant lacked standing to challenge GPS device tracking, but that even with standing *Knotts* controlled in such a way as preclude the warrant requirement for GPS tracking), United States v.

decided in favor of the petitioner on the comparatively mundane ground of trespass to chattels, with a five-Justice opinion authored by Justice Scalia holding that the physical alteration of Jones's car occasioned by the placement of the GPS tracker constituted a per se violation of the Fourth Amendment irrespective of the traditional *Katz* analysis.[71]

Justice Alito, authoring a four-Justice concurrence in judgment that was in many respects effectively a dissent,[72] argued similarly to the *Maynard* court that prolonged surveillance was precluded by *Katz*, and that *Knotts* sanctioned only relatively short-term surveillance.[73] The precise amount of time for which surveillance was authorized was a matter for future resolution by the judiciary or legislatures, but the four weeks at issue in *Jones* were surely too long:

> [S]ociety's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period. In this case, for four weeks, law enforcement agents tracked every movement that respondent made in the vehicle he was driving. We need not identify with precision the point at which the tracking of this

Pineda-Moreno, 591 F.3d 1212, 1216 (9th Cir. 2010), *vacated*, 132 S. Ct. 1533 (2012) (warrantless GPS tracking not a search under *Knotts*), *and* United States v. Garcia, 474 F.3d 994 (7th Cir. 2007) (warrantless GPS tracking not a search under *Knotts*). The D.C. Circuit in *Maynard* took some support for its reliance on the "twenty-four hour surveillance" language of *Knotts* from a footnote in a Fifth Circuit opinion that, although ultimately finding that conduct similar to that in *Jones* did not warrant suppression, nevertheless felt it appropriate to hew to the reservation of wholesale surveillance alluded to in *Knotts*. *Maynard*, 615 F.3d at 557 (citing United States v. Butts, 729 F.2d 1514, 1518 n.4 (1984)). It is noteworthy that the Fifth Circuit's opinion in *Butts* applied with respect to aircraft, whose comings and goings, the Fifth Circuit noted, are generally subject to much more comprehensive oversight than those of cars. *Butts*, 729 F.2d at 1517 (citing United States v. Bruneau, 594 F.2d 1190, 1196 (8th Cir. 1979)).

70. 132 S. Ct. 945 (2012).

71. *Id.* at 951–52.

72. Although Justice Alito concurred with the majority that the police conduct at issue constituted a Fourth Amendment search, he strongly opposed the rationale the Court used to justify its decision, believing "18th-century tort law" ill suited to the resolution of issues raised by a "21st-century surveillance technique." *Id.* at 957–58 (Alito, J., concurring) ("This holding, in my judgment, is unwise. It strains the language of the Fourth Amendment; it has little if any support in current Fourth Amendment case law; and it is highly artificial.").

73. *See id.* at 964 (citing United States v. Knotts, 460 U.S. 276, 281–82 (1983)) ("Under [existing Fourth Amendment doctrine], relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable.").

> vehicle became a search, for the line was surely crossed before the 4-week mark.[74]

Justice Sotomayor, who joined the majority, also authored a single-Justice concurrence that contained elements of both the Scalia and Alito opinions.[75] She agreed with Justice Scalia that because a constitutional guarantee against warrantless trespass to chattels was sufficient to decide the case such a parsimonious holding was appropriate.[76] However, Justice Sotomayor also wrote at length about the concerns evinced by the *Maynard* opinion and by Justice Alito's concurrence:

> GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. The Government can store such records and efficiently mine them for information years into the future. And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: limited police resources and community hostility.[77]

Although the official holding of the *Jones* case is limited to the Fourth Amendment's applicability to trespass to chattels, five of the nine Justices endorsed a reading of the Fourth Amendment that acknowledges that the *quantity* of information obtained—not simply the *procedures used* in obtaining it—is capable of infringing on the "reasonable expectation of privacy" that forms the backbone of

74. *Id.*

75. *Id.* at 954 (Sotomayor, J., concurring).

76. *Jones*, 132 S. Ct. at 954 (Sotomayor, J., concurring).

77. *Id.* at 955–56 (internal quotation marks and citations omitted). Judge Kozinski had expressed similar concerns in his dissent to denial of en banc rehearing in *Pineda-Moreno*. United States v. Pineda-Moreno, 617 F.3d 1120, 1125 (9th Cir. 2010) (Kozinski, J., dissenting) ("By tracking and recording the movements of millions of individuals the government can use computers to detect patterns and develop suspicions. It can also learn a great deal about us because where we go says much about who we are. Are Winston and Julia's cell phones together near a hotel a bit too often? Was Syme's OnStar near an STD clinic? Were Jones, Aaronson and Rutherford at that protest outside the White House?").

present-day Fourth Amendment analysis.[78] In the view of a Court majority, then, "quantity has a quality all its own."[79]

*F. The Post-*Jones *Horizon and Its Problems: Whither Procedure?*

The "quantity matters" thread in *Jones* became more concrete in *Riley v. California*, in which all justices save Alito (who concurred in part and concurred in judgment) concluded that a warrantless search of a cellular phone in an arrestee's possession violated the Fourth Amendment despite the broad discretion afforded officers in conducting a search incident to arrest, under which items on an arrestee's person would prima facie be subject to search without the need for a warrant.[80] Although the majority opinion made some allusion to unique features of smartphones, it rested its holding primarily on the simple fact that modern phones can contain a great deal of data.[81] The Court held that the amount of data available (in particular routinely available) on smartphones created a difference between a phone and, for example, a personal journal, that was categorical rather than merely one of degree.[82] Although *Riley* per se has limited implications for public surveillance (pertaining as it does to personal phones), it affirms that a Court majority is willing to accept the proposition intimated in *Jones* that the quantity of information disclosed by a search can be an independent Fourth Amendment gravamen even if the search itself would not require a warrant based solely on its procedural guise.

78. As Orin Kerr observes, the fact that five of nine Justices have expressed significant concern about technological compromise of substantive privacy rights may well indicate that significant changes are to come in this area of the law. Kerr, *supra* note 50, at 326–28 ("[F]ive justices wrote or joined opinions that did touch on the mosaic theory. Their opinions are somewhat cryptic, but they suggest that a majority of the Court is ready to embrace some form of the D.C. Circuit's mosaic theory.").

79. This quote has been variously attributed to both Stalin and Lenin. *Compare* Robert M. Gates, Sec'y of Def., Speech at the Naval War College (Apr. 17, 2009) ("As Stalin once said, 'Quantity has a quality all of its own.'"), *with* CONGRESSIONAL BUDGET OFFICE, EFFECT OF WEAPONS PROCUREMENT STRETCH-OUTS ON COSTS AND SCHEDULES 2 (1987), *available at* http://www.cbo.gov/sites/default/files/doc21b-entire.pdf ("As Lenin put it, 'Quantity has a quality all its own.'").

80. 134 S. Ct. 2473, 2479–85 (2014) (quoting United States v. Robinson, 414 U.S. 218, 235 (1973)) ("[A] 'custodial arrest of a suspect based on probable cause is a reasonable intrusion under the Fourth Amendment; that intrusion being lawful, a search incident to the arrest requires no additional justification.'").

81. *Id.* In particular, the Court highlighted the fact that smartphones may be able to access data physically "at home" on a remote server (such as an e-mail account), thus extending a search's reach far beyond the contents of the phone at issue. *Id.* at 2491.

82. *Id.* at 2490.

The tensions engendered by a quantity- or content-based reconceptualization of *Katz* are readily apparent. The Alito and Sotomayor "quantity matters" opinions in *Jones* and the majority holding in *Riley* express concerns that, unless people resort to secret-agent level attempts at elusion, everything they do risks being subject to governmental scrutiny *de facto* and not merely in an abstract and typically unrealized sense *de jure*. Surveillance proliferation threatens previous expectations that persons of no present interest will be ignored entirely by the government. Thus ubiquitous surveillance undermines the so-called "right to be let alone."[83]

Such concerns, however, must be read against the backdrop of *Katz* and its progeny, and in particular the repeated statements that what is "knowingly exposed to the public" is not an appropriate subject of Fourth Amendment protection.[84] The Fourth Amendment is historically conceptualized as a procedural limit on police authority to conduct searches.[85] In other words the existence of a warrant requirement is predicated on whether a specific activity, procedurally speaking, is or is not a search.[86] Since simply recording publicly disclosed data has been consistently held not to constitute a search,[87] a "content matters" standard wreaks a tremendous sea

83. Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting); *see also* Katz v. United States, 389 U.S. 347, 350–51 (1967) (arguing that the general "right to be let alone" is best protected by the states).

84. *See* discussion *supra* Part I.B.

85. *See, e.g.*, Kerr, *supra* note 50, at 312 (arguing that the threshold question in Fourth Amendment jurisprudence is whether or not an action or series of actions constitutes a "search"); *see also Riley*, 134 S. Ct. at 2491–92 (discussing the "general preference to provide clear guidance to law enforcement through categorical rules").

86. *See* Kerr, *supra* note 50, at 312.

87. *E.g.*, United States v. Caceres, 440 U.S. 741, 755 (1979) (holding recording a conversation not to be a Fourth Amendment violation); United States v. White, 401 U.S. 745, 751 (1971) (plurality opinion) ("If the conduct and revelations of an agent operating without electronic equipment do not invade the defendant's constitutionally justifiable expectations of privacy, neither does a simultaneous recording of the same conversations made by the agent or by others from transmissions received from the agent to whom the defendant is talking and whose trustworthiness the defendant necessarily risks."); Lopez v. United States, 373 U.S. 427, 440 (1963) (describing the admissibility of a recording by an informant and stating that it was admissible as a result of the lack of violation of substantive rights in obtaining the statement: "The function of a criminal trial is to seek out and determine the truth or falsity of the charges brought against the defendant. Proper fulfillment of this function requires that, constitutional limitations aside, all relevant, competent evidence be admissible, unless the manner in which it has been obtained—for example, by violating some statute or rule of procedure—compels the formulation of a rule excluding its introduction in a federal court."). Indeed it seems intuitively obvious that recording publicly disclosed data

change in the judicial conception of what the Fourth Amendment is meant to actually *do*.

Orin Kerr has argued (writing prior to *Riley*) that reconceptualizing the Fourth Amendment to focus on the *substantive information* revealed by government actions instead of on the *procedural character* of those actions not only fundamentally subverts preexisting Fourth Amendment doctrine, but also poses such significant line-drawing problems that a hasty retreat from the Sotomayor and Alito *Jones* opinions is in order.[88] Roughly speaking the argument goes something like this: even if the *Maynard* court and a majority of the Supreme Court are correct that a purely procedural conception of Fourth Amendment searches allows technology to eat away at the substantive right to privacy, the need for clarity in conduct rules that police actually follow on a day-to-day basis is fundamentally at odds with the nebulous character of questions like "how much information is too much?"[89]

Kerr's approach, however, mischaracterizes the problem. The difficulty is not only that procedural rules have failed to protect the substantive right to privacy, but that in fact the basic bounds of the substantive right itself are ill defined. There is as yet no obvious, bright line which, when crossed, allows courts to say "here, at this point, privacy is violated."

---

is not a search. *See* Kerr, *supra* note 50, at 312 ("If no individual step in a sequence counts as a search, then the Fourth Amendment is not triggered. No Fourth Amendment violation has occurred."). Although the Supreme Court has held that the collation of data may represent an independent form of privacy breach, it has thus far only done so in the context of a statute explicitly ordaining that respect for privacy be weighed against the public interest in the release of criminal records. *See, e.g.*, U.S. Dep't. of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 762–63 (1989); *see also supra* note 62 and accompanying text. To date no constitutional opinion has held that the collation of data from a series of non-searches can itself be a search. *Cf.* Fred F. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 HARV. C.R.-C.L. L. REV. 435, 437 (2008). Indeed the obvious reading of *Knotts* would seem to preclude this conclusion. *See* United States v. Knotts, 460 U.S. 276, 281 (1983) (treating as dispositive the fact that the total set of passersby taken as a whole would have been aware of defendant Petschen's whereabouts). *See generally supra* note 36 and accompanying text.

88. Kerr, *supra* note 50, at 344. *Riley* notably explicitly reserved the question of whether "mosaic searches" were a form of independent search, perhaps out of caution on the Court's part vis-à-vis the line-drawing concerns discussed above. *Riley*, 134 S. Ct. at 2489 n.1 ("Because the United States and California agree that these cases involve searches incident to arrest, these cases do not implicate the question whether the collection or inspection of aggregated digital information amounts to a search under other circumstances.").

89. Kerr, *supra* note 50, at 344, 346–47; *see also Riley*, 134 S. Ct. at 2491–92 (discussing preference for categorical rules to guide law enforcement conduct).

The remainder of this Note argues that this problem is best solved not by insistence on a return to preexisting search doctrine, but instead by giving privacy (and its attendant reasonable expectations) a more concrete definition. Once the threshold of what constitutes a privacy breach has been established, that definition may be used to create a constitutional theory of the ubiquitous surveillance of public space that steers clear of crossing the line.

II.
ADAPTING *KATZ* TO THE CHANGING TECHNOLOGICAL LANDSCAPE: THE NEED TO DEFINE PRIVACY IN ORDER TO AFFORD IT APPROPRIATE PROTECTIONS AGAINST UBIQUITOUS SURVEILLANCE

The object of this Note is to develop a theory and set of rules for the regulation of large-scale—that is, ubiquitous—surveillance of public spaces,[90] and of the collation of information gathered therefrom.[91] A majority of the Court agrees that the scale of comprehensive surveillance implicates novel Fourth Amendment concerns despite previous holdings that public activities are outside the Fourth Amendment's protection.[92] The scope of information subject to collection by modern technology creates a difference in *kind* rather than merely *degree*.[93] But the Court has yet to articulate pre-

90. This Note generally uses "public surveillance" and related terms to refer to the collection, recording, and/or collation of data that is nominally public or publicly available; for instance, recording all passersby on a public thoroughfare, drawing inferences based on public records, or recording and cross-referencing all license plate numbers of cars using a public road. However, this Note's analysis is extensible to information that is not arguably of a public character but which nevertheless may be subject to widespread government data gathering and analysis such as, for example, the NSA's phone-metadata gathering program.

91. Though this Note will attempt to address ubiquitous surveillance in both the routine law enforcement and domestic intelligence-gathering contexts, the emphasis will be primarily on law enforcement, in part due to the greater role of public courts in administering Fourth Amendment compliance with respect to law enforcement than with respect to the intelligence services. *See* ACLU v. Clapper, 959 F. Supp. 2d 724, 730 (S.D.N.Y. 2013) (quoting United States v. U.S. Dist. Court (*Keith*), 407 US. 297 (1972)) ("[I]n 1972, the Supreme Court recognized that 'criminal surveillances and those involving domestic security' are distinct, and that 'Congress may wish to consider protective standards for the latter which differ from those already prescribed for [criminal surveillances].'").

92. *See supra* Part I.E.

93. *See, e.g.*, *Riley*, 134 S. Ct. at 2493 ("But the fact that a search in the pre-digital era could have turned up a photograph or two in a wallet does not justify a search of thousands of photos in a digital gallery. The fact that someone could have tucked a paper bank statement in a pocket does not justify a search of every bank statement from the last five years.").

cisely how such a view is compatible with either the long pedigree of Fourth Amendment jurisprudence post-*Katz* or the essentially procedural orientation of the Fourth Amendment warrant requirement.

The Court's failure to define privacy per se has led to a mischaracterization of what interests are at stake with respect to ubiquitous surveillance and, in particular, *when* they are at stake. Modern surveillance technology fundamentally changes the appropriate metaphors that apply to search doctrine,[94] and this has led to the present confusion about ubiquitous data collection's capacity for *substantive* privacy compromise despite its *procedural* validity. Ubiquitous data collection and collation searches are simply not procedurally analogous to the types of searches conducted by living, breathing police. Rather, although ubiquitous surveillance infrastructure has an incalculably greater capacity to gather data, it need not in fact implicate the *Katz* test in and of itself.[95] Ironically the sheer volume of available information dwarfs the capacity of human beings to view, or even care about, the overwhelming majority of it.[96]

A consideration of what, precisely, privacy *is*—and, in particular, when it is compromised—demonstrates that Fourth Amendment protections should properly attach to data *access* instead of data *gathering*, and that rather than focusing on how much data is too much, the correct place to focus Fourth Amendment protec-

94. Justice Alito's *Jones* concurrence in judgment rather acerbically alludes to the strains that technology puts upon preexisting search metaphors; referring to the analogy of GPS vehicle tracking to a constable secreting himself in a target's coach, Justice Alito observes, "[t]he Court suggests that something like this might have occurred in 1791, but this would have required either a gigantic coach, a very tiny constable, or both—not to mention a constable with incredible fortitude and patience." United States v. Jones, 132 S. Ct. 945, 958 n.3 (2012) (Alito, J., concurring).

95. *But see* United States v. Maynard, 615 F.3d 544, 561–62 (D.C. Cir. 2010), *aff'd in part sub nom. Jones*, 132 S. Ct. 945 (arguing that qualitative changes in the information disclosed by prolonged surveillance represent a new form of privacy harm); *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring) (arguing that unique attributes of low-cost, technologically facilitated information gathering need to be accommodated into the *Katz* analysis).

96. This problem is not a new one in the national security space. Shane Harris, discussing the development of surveillance infrastructure at the NSA in the early 2000s, points out that a persistent early problem of ubiquitous surveillance attempts was that the quantity of incoming data would far outstrip the agency's capacity to analyze it, even by automation. SHANE HARRIS, THE WATCHERS 208–09 (2010); *see also supra* note 79 and accompanying text.

tion is on the Google main page and its law enforcement equivalents.

A. Shouting Down the Well: Disclosure, Breach, and the Separability of the Two

The Supreme Court's treatment of the *Katz* test has thus far focused exclusively on the existence or nonexistence of the "reasonable expectation" in question, rather than attempting to give content to what exactly privacy is.[97] In times past this was a defensible course: unlike concepts such as "free will," which live or die by their definitions,[98] first-stab definitions of privacy are relatively easy to formulate and, for many Fourth Amendment purposes, perfectly serviceable.[99] In fact a minimalist definition of privacy may be salutary as a general matter. By focusing Fourth Amendment analysis on the "reasonable expectation," the Court can protect substantive rights without attempting to create a set-in-stone definition of privacy subject to constant amendment in later cases that risks ultimately ending up a tangled verbal and semantic morass riddled with individual exceptions.[100] By invoking "reasonable expecta-

97. Katz v. United States, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring); *see also* California v. Greenwood, 486 U.S. 35, 41 (1988) (emphasis added) ("Our conclusion that society would not accept as reasonable respondents' claim to *an expectation of privacy* in trash left for collection in an area accessible to the public is reinforced by the unanimous rejection of similar claims by the Federal Courts of Appeals."); California v. Ciraolo, 476 U.S. 207, 214 (1986) ("On this record, we readily conclude that respondent's expectation that his garden was protected from such observation is unreasonable and is not an expectation that society is prepared to honor."); *supra* note 5 and accompanying text.

98. *See, e.g.*, GREGG D. CARUSO, FREE WILL AND CONSCIOUSNESS: A DETERMINIST ACCOUNT OF THE ILLUSION OF FREE WILL 8–10 (2012) (discussing difficulty of reconciling "folk-psychological" accounts of concepts like "autonomy," "self-control," and "ability to do otherwise" with an essentially deterministic account of the macro-physical universe that seems to rob them of content).

99. In this respect, an analogy could be drawn between the Court's deliberately nebulous conception of privacy and Justice Stewart's famous refusal to provide a precise definition of "obscenity":

> I shall not today attempt further to define the kinds of material I understand to be embraced within that shorthand description [of obscenity]; and perhaps I could never succeed in intelligibly doing so. But I know it when I see it, and the motion picture involved in this case is not that.

Jacobellis v. Ohio, 378 U.S. 184, 197 (1964) (Stewart, J., concurring).

100. Arguably search doctrine has in fact developed exactly this sort of Swiss cheese problem in the form of various and sundry tests for what is and is not a search in the automobile context. *See, e.g.*, California v. Acevedo, 500 U.S. 565, 579–80 (1991) (explicitly overruling *Sanders* and implicitly abrogating *Chadwick* while holding that the scope of probable cause limited to a container within an automobile does not justify a search beyond that container); United States v. Ross,

tions" rather than the meaning of "privacy" per se, the Court can find recourse in a more objective (albeit mutable) standard of judgment—the privacy expectations of typical members of society—as well as avoid a prolonged and often unnecessary excursion into a semantic quagmire.[101] Whatever the exact contours of privacy are in a philosophical sense, there has nevertheless been broad societal agreement that a police officer riffling through one's person, papers, or effects represents an infringement of it.[102]

B. Disclosure Versus Breach

What happens, however, when the papers and effects are stored and made available to the police but never in fact *accessed*? In a world of ubiquitous surveillance this is not only a hypothetical *possibility* but frequently a physical *necessity*.[103] The sheer volume of data routinely now available to law enforcement dwarfs the human capacity to view it, let alone analyze it.[104] As the current Google

456 U.S. 798, 822 (1982) (extending probable cause to containers when police have probable cause with respect to car in general); Arkansas v. Sanders, 442 U.S. 753, 765 (1979) (extending *Chadwick* to automobiles in motion); United States v. Chadwick, 433 U.S. 1, 8 (1977) (refusing to extend probable cause for a stopped automobile to closed containers *within* that car); Carrol v. United States, 267 U.S. 132, 162 (1925) (holding warrant not required for automobile searches). Justice Scalia recently adverted to the incoherence of automobile search doctrine in his dissenting opinion in *Maryland v. King*: "Compare, *New York v. Belton*, 453 U. S. 454 (1981) (suspicionless search of a car permitted upon arrest of the driver), with *Arizona v. Gant*, 556 U. S. 332 (2009) (on second thought, no)." 133 S. Ct. 1958, 1990 n.6 (2013) (Scalia, J., dissenting) (citations omitted).

101. *Cf.* United States v. Jones, 132 S. Ct. 945, 954 (2012) (arguing that delaying the categorical resolution of thorny problems in fast-changing technological landscapes may itself be a meritorious approach).

102. *See* U.S. CONST. amend. IV (protecting "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures").

103. *See, e.g.*, Randy Rieland, *Big Data or Too Much Information?*, SMITHSONIAN (May 7, 2012), http://www.smithsonianmag.com/innovation/big-data-or-too-much-information-82491666/?no-ist ("By last year, we were cranking out [five billion gigabytes of data] every two days. By next year . . . we'll be doing it every 10 minutes. . . . It's the latest example of technology outracing our capacity to use it."); *see also, e.g.*, Julia Angwin, *NSA Struggles to Make Sense of Flood of Surveillance Data*, WALL ST. J. (Dec. 25, 2013, 10:30PM), http://www.wsj.com/articles/SB10001424052702304202204579252022823658850 (reporting claims that the NSA analysts were "swamped with so much information that they c[ouldn]'t do their jobs effectively" and citing an internal NSA document acknowledging that efforts to track foreign cellphone location were "outpacing [the NSA's] ability to ingest, process and store" data).

104. *See, e.g.*, Angwin, *supra* note 103. The same issues facing the NSA are likewise a concern for more typical law enforcement agencies. Police departments

share price attests,[105] when information is available in sufficiently high volumes, the capacity to extract anything of value from massive amounts of data is dependent upon the ability to index and search it efficiently.[106] In high-data availability environments any sort of purely nominal idea of the availability of information is belied by the practical impossibility of searching it line by line.[107]

The significance of this cornucopia of information is that, in contrast to ages past, the advent of technology has enabled the separation of the *disclosure* of putatively private information from the *breach* of the privacy interest in that information. Consider the idea of shouting one's deepest, most personal secrets down an abandoned, empty well: there is unquestionably a disclosure of information, but with no one to listen to it, there has been no compromise of privacy.

With this understanding in hand it becomes necessary to move beyond the nebulous concept of privacy that has been the background presumption of previous cases. The result of an insufficiently nuanced definition of privacy has been a line of cases that

in Los Angeles, for instance, had approximately 160 million unique logs of the locations and license plate numbers of cars on public streets as of June 2012, which could be cross-referenced with known criminal acts to facilitate locating a suspect. Jon Campbell, *License Plate Recognition Logs Our Lives Long Before We Sin*, L.A. WEEKLY (June 21, 2012), http://www.laweekly.com/2012-06-21/news/license-plate-recognition-tracks-los-angeles/full/.

105. As of December 30, 2014, the Google share price was $530.66 and its market capitalization was $360.39 billion. *Google Shares Outstanding*, YCHARTS, http://ycharts.com/companies/GOOG/shares_outstanding (last visited Apr. 23, 2015) (stating that Google had 680.17 million shares outstanding as of December 31, 2014); *Historical Prices for Google Inc. on Dec. 31, 2014*, GOOGLE FINANCE, https://www.google.com/finance/historical?cid=694653&startdate=dec+31%2C+2014&enddate=dec+31%2C+2014&num=30&ei=Tkc5VcGQOYausQen2oDQCw (last visited Apr. 23, 2015). "Market capitalization is calculated by multiplying a company's shares outstanding by the current market price of one share. *Market Capitalization*, INVESTOPEDIA, http://www.investopedia.com/terms/m/marketcapitalization.asp (last visited Apr. 23, 2015).

106. *Cf.* Sergey Brin & Lawrence Page, *The Anatomy of a Large-Scale Hypertextual Web Search Engine*, COMPUTER NETWORKS AND ISDN SYSTEMS, Apr. 1998, at 107, 109, *available at* http://ilpubs.stanford.edu:8090/361/1/1998-8.pdf.

107. Douglas Adams, in his famous novel *The Hitchhiker's Guide to the Galaxy*, eloquently highlighted the distinction between nominal availability of information and practical access thereto in a scene in which protagonist Arthur Dent, facing the bulldozing of his home to make way for a highway bypass, responds to a bureaucrat's contention that the information was public knowledge: "'But look, you found the notice didn't you?' 'Yes,' said Arthur, 'yes I did. It was on display in the bottom of a locked filing cabinet stuck in a disused lavatory with a sign on the door saying 'Beware of the Leopard.'" DOUGLAS ADAMS, THE HITCHHIKER'S GUIDE TO THE GALAXY 10 (Random House 1997) (1980).

have equated data gathering with the warrant protection requirement that in fact more properly inheres in data access and analysis.[108]

C. A (Partial) Definition of Privacy: The Human Observer as Sine Qua Non

This Note does not propose to provide a uniform definition of privacy. Such a semantic signpost would likely have many of the same qualities now that have made an explicit definition undesirable in the past.[109] Rather it is possible to infer some of the properties of privacy without hashing out its precise contours in their entirety. This Note proposes that one such property is what shall hereafter be referred to as the "Human Observation" or "Human Observer" test: in order for privacy to be breached, a human observer must be aware of the personal information whose character is sought to be kept private.[110]

To previous courts this proposition probably would have seemed so obvious that it would have been laughably unnecessary to spell it out.[111] More importantly it would have been an utterly

108. Commentators have not ignored the possibility that use, rather than gathering, restrictions may be more suited to the modern age of computerized data-gathering. *E.g.*, ORIN S. KERR, USE RESTRICTIONS AND THE FUTURE OF SURVEILLANCE LAW 7–8 (2011), *available at* http://www.brookings.edu/~/media/research/files/papers/2011/4/19%20surveillance%20laws%20kerr/0419_surveillance_law_kerr.pdf. In fact Admiral John Poindexter's work on the Defense Advanced Research Project Agency's (DARPA) Total Information Awareness (TIA) data mining system in the early 2000s included a proposed set of use restrictions on access to sensitive personal data even as the essence of the system included pouring all possible information into it. HARRIS, *supra* note 96, at 190 ("[T]he farther into the data a user wished to probe, the more outside authority he had to obtain."). This Note's specific contribution to the argument is fitting a conceptualization of the heretofore undefined notion of privacy in *Katz* into the *constitutional* argument for a use-restriction oriented approach to ubiquitous surveillance.

109. *See supra* note 100 and accompanying text.

110. This definition has been embraced by other commentators who note the fact that it is only recent technological innovations that make it interesting. *See* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 551 (2005) (arguing that in the computer search context "a search occurs when information from or about the data is exposed to possible human observation, such as when it appears on a screen, rather than when it is copied by the hard drive or processed by the computer"); Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 612–19 (2011) (discussing the human observer theory of privacy).

111. *See* Tokson, *supra* note 110, at 616 (noting the need to make explicit what was merely "implicit" in previous judicial opinions dealing with Fourth Amendment privacy).

academic, essentially useless distinction to highlight. As evidenced most recently by Justice Alito's *Jones* opinion, in a world where the dominant allegory of what constitutes a search is a constable physically searching one's effects (or, in the case of *Jones*, tailing your carriage), there cannot be a disclosure of information to the government without such information being disclosed to a human observer—that is, to the constable him- or herself.[112] The breach of privacy is implicit in the means of disclosure. However, the context of *Jones* makes it equally evident that the constable-as-allegory is just that: an allegory.[113] The present nature of on-the-ground data gathering—for instance, by attaching a GPS tracker to Jones's car so that its data can be reviewed and checked later—emphasizes the separability of the *disclosure* of putatively private information from the *breach* of the privacy interest associated therewith. Gathering nominally public data can be a purely automated process. *Looking at it* subjects the target of observation to the same threats of judgment and censure that that have so agitated courts concerned with ubiquitous surveillance.[114]

III.
IMPLICATIONS OF THE HUMAN OBSERVATION TEST FOR WARRANTS AND UBIQUITOUS SURVEILLANCE: USE RESTRICTIONS TRUMP GATHERING RESTRICTIONS

Despite its relative parsimony the notion that a privacy breach is only triggered at the point of human involvement creates some natural first principles for the development of a constitutional search doctrine that recognizes the distinction between privacy breach and information disclosure. These first principles include the following:

First, the Human Observation test is only relevant as applied to data that has been passively gathered and is subject to review after the fact.

Second, any amount of active human review, in general, represents a Fourth Amendment search subject to warrant protection. However, information to which the government would already have

112. *See* United States v. Jones, 132 S. Ct. 945, 958 (2012) (Alito, J., concurring) ("[I]t is almost impossible to think of late-18th-century situations that are analogous to what took place in this case. (Is it possible to imagine a case in which a constable secreted himself somewhere in a coach and remained there for a period of time in order to monitor the movements of the coach's owner?)").

113. *Id.* (criticizing the constable allegory as inapposite to current state of technology).

114. *See supra* note 77 and accompanying text.

had access ("administrative" information) and information needed to identify the target of a search is exempted from the warrant requirement.

Third, all ex ante information gathering by law enforcement of data within the public domain is prima facie constitutional and has no attendant warrant protections for so long as it is not viewed by a law enforcement agent.

Each of these implications is elaborated on below.

A. Principle One: Applicability of the Human Observation Test

The Human Observation test is only relevant in cases involving passively gathered data that is subject to review after the fact, and not in cases involving direct evidence gathering by a human police officer. This is because in the latter cases the evidence gathered will be known to at least the officer who gathered the information in the first place. Because the Human Observation test will therefore always be satisfied in cases involving direct, human evidence-gathering, requiring "exposure to human observation" as a condition precedent to privacy breach adds nothing to existing jurisprudence. By contrast in cases where information has been passively gathered using some form of technology, exposure to human observation is not a given. Instead the human observation test is only satisfied in such cases when a human law enforcement (or intelligence) officer has actually reviewed the passively gathered, technologically sourced data

Within cases involving passively gathered data the Human Observation test becomes relevant only where that data is subject to being reviewed—or not—after the fact. It is not relevant in cases where such data is actively and continuously monitored (for example, in cases where municipal surveillance cameras are actively monitored). Limiting the applicability of the Human Observation test to situations where passively gathered data may or may not be reviewed by police makes sense in light of the idea that any kind of active human involvement is subject to the practical constraints of "limited police resources" that have concerned courts about ubiquitous surveillance.[115] Active and continuous monitoring of passively gathered data does not necessitate a new privacy framework in the way that ex post review of such data does.

115. United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) (citing Illinois v. Lidster, 540 U.S. 419, 426 (2004)).

B. Principle Two: The Human Observation Test's General Applicability and the Scope of Pragmatic Exceptions to the Warrant Requirement

One of the chief virtues of the Human Observation test is that it provides a bright-line rule to law enforcement[116]: if a human is reviewing information gathered by means of ubiquitous surveillance infrastructure then it is by definition subject to warrant protection.[117] Because the *Katz* test protects "reasonable expectations of privacy,"[118] and the access of data is a sine qua non of a privacy breach, the act of access itself—in essence the law enforcement analogue of hitting "enter" on a Google search—is the place at which warrant protections attach.

A substantial amount of present and historical law enforcement practice, however, consists of reviewing already-gathered information.[119] Insofar as ubiquitous surveillance raises no new *Katz* privacy concerns with respect to information available in previous technological eras, it is logical to preserve the constitutional status quo. Such preservation implies the need for pragmatic exceptions to the rule that any human review of passively gathered data represents a privacy breach in need of warrant protection. This Note proposes two such exceptions.

1. Administrative Information

The first exception to the "if human access, then warrant" requirement is for purely administrative data already within the possession of governmental authorities.

---

116. *Cf. id.* at 954 (Scalia, J.) (discussing difficulties of line drawing based on the duration of surveillance).

117. *Cf.* Kerr, *supra* note 110, at 552 (noting that, with respect to searches of computers, a human observer-centric privacy model is much easier to administer than one that has to account for the precise inner workings of computational components).

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

119. *See* Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. PA. L. REV. 327, 360 (2015) (discussing police use of records of past convictions, arrests, addresses, and other information stored in large computerized databases); Stephen Mercer & Jessica Gabel, *Shadow Dwellers: The Underregulated World of State and Local DNA Databases*, 69 N.Y.U. ANN. SURV. AM. L. 639, 670 (2014) (discussing police use of DNA databases); William H. Rehnquist, *Is an Expanded Right of Privacy Consistent with Fair and Effective Law Enforcement?*, 23 KAN. L. REV. 1, 8 (1974) ("Law enforcement authorities likewise utilize records of arrest when reaching a number of discretionary decisions they are regularly called on to make, including whom to investigate, whom to charge with what, and what sentence or parole terms to advocate.").

The government's ability to access administrative data—vital statistics such as those appearing on a driver's license, birth certificate, or social security card—has for so long been a background presumption of American life that it seems to warrant a per se lack of cognizable privacy interest.[120] To put it in the language of *Katz*, persons generally possess neither a subjective expectation of privacy in government records vis-à-vis the government[121] (because the government already possesses such records) nor would any such expectation of privacy be objectively reasonable (for the same reason).

Moreover such data generally fails to meet even the requirement of passive acquisition[122]: typically administrative information is either volunteered by a citizen (for instance, at the DMV) or actively collected (for instance, weight at birth). In other words it falls under existing jurisprudence because it is not the product of passive surveillance subject to ex post review.[123] The administrative information exception is intended to be uncontroversial. Essentially it serves the interest of avoiding formalistic restrictions on the access of data that may be passively gathered but which has historically been considered categorically available to state actors.

2. Identificatory Information

A somewhat thornier problem is presented by "identificatory" data—that is, data required to identify the individual to whom some passively gathered record pertains.[124] As a preliminary matter it is essential to draw a distinction between information that identifies the individual subject of a record and records about an already-identified individual. In order for information to properly be identificatory, it must only be used to match a record to a subject, and not the other way around. The latter category of information—a search for government records pertaining to the comings and go-

120. *Cf.* Smith v. Maryland, 442 U.S. 735, 743–44 (1979) (individuals do not retain privacy interest in information voluntarily turned over to third parties).

121. Of course they may still have a cognizable expectation that such records will not be disclosed to the general public, as would be the case with, for example, Social Security Numbers. *See, e.g.*, U.S. Dep't of Justice v. Reporters Comm. for Freedom of Press, 489 U.S. 749, 762–63, (1989) (holding that criminal rap sheets, despite being compilations of public records maintained by the government, are not per se subject to FOIA disclosure).

122. *See supra* Part II.B.

123. *See id.*; *see also supra* Part III.A (discussing applicability of Human Observation test only to passively gathered data subject to ex post review).

124. Such data includes, for instance, the various sources, public and private, used to identify perpetrators of the Boston Marathon bombings. *See supra* note 10 and accompanying text.

ings of a known person—runs directly afoul of the concerns voiced by various current and former Justices about the capacity for surveillance to compromise privacy expectations previously guaranteed by practical obscurity.[125] Accordingly this Part deals only with the information needed to match an individual to a record and not the other way round.[126]

Unlike the essentially mundane nature of administrative records, identificatory data may well have a character that would be of great independent interest to law enforcement or the trier of fact. For instance, although there was no question in their immediate aftermath about whether the Boston bombings had occurred, discerning the bombers' identity was central to the resultant law enforcement response.[127] Similarly review of footage of a mugging or assault may be used to identify the assailant in a case in which the fact of the assault or mugging is largely uncontested, thus cutting off a primary, otherwise-contestable avenue of defense: mistaken identity. Unlike a defendant's social security number or the address on her driver's license, identificatory data has significant potential to materially incriminate a defendant in the same manner as information more traditionally subject to Fourth Amendment protection and the exclusionary rule. Nevertheless despite its potential use for substantive incrimination in addition to identification, such identificatory data should be exempted from the warrant requirement just as administrative data should.

The need for identification is, as a practical matter, indispensable. Given certain identifying characteristics of a criminal suspect, the need to index these characteristics to his or her identity is essential to any kind of effective law enforcement or intelligence action. Moreover without knowing who a criminal suspect identified in a surveillance video or suspicious metadata record is, issuing any

125. *See, e.g.*, United States v. Jones, 132 S. Ct. 945, 955–56 (2012) (Sotomayor, J., concurring) (expressing concern about the kind of "mosaic" theory harms represented by collation of continuously gathered GPS data); United States v. Knotts, 460 U.S. 276, 283–84 (1983) (describing "24-hour surveillance" concerns); *see also Reporters Comm. for Freedom of Press*, 489 U.S. at 762 (holding that FOIA does not compel disclosure of federally compiled "rap sheets" and observing that there is a privacy interest in "practical obscurity").

126. A canonical example of this type of search would be identifying a car's owner based on speed camera footage of its license plate.

127. Seelye et al., *supra* note 3 (reporting that "[o]fficials said they have images of one of the men putting a black backpack on the ground just minutes before two near-simultaneous blasts went off near the finish line of the marathon at 2:50 p.m. on Monday" and quoting an official as saying that "the nation is counting on those with information [about who the men are] to come forward and provide it to [law enforcement authorities]").

kind of search or arrest warrant is effectively impossible. As such indexing a criminal suspect's identifying characteristics to his or her identity should be treated as a presumptively valid exercise of law enforcement authority that ought not, in and of itself, come under the auspices of the Fourth Amendment. Much as identification of suspects (for instance, from a lineup) is not dependent on warrant acquisition, neither should a warrant be required for the identification of suspects from ubiquitous surveillance data.

Despite identificatory data's pragmatic indispensability in the context of criminal investigation, the potential compromise of public anonymity certainly has implications not just for those constitutional concerns traditionally protected by the exclusionary rule but also for the sort of generalized privacy concerns evinced by ubiquitous surveillance. Absent a link to a particular indexical identity, various disparate aspects of public surveillance do not present the same "24-hour surveillance" risk as that alluded to in Justice Sotomayor's *Jones* concurrence.[128] The distinction would be between government knowing that someone has entered a strip club—someone whose identity is likely only known to law enforcement if the entrant is already a person of interest—and government knowing that Jonathan C. Doe, of 24 West Park Street, Cleveland, Ohio, has entered a strip club. Unlike administrative data, then, identificatory data represents a substantive change in the background presumptions that citizens maintain about which activities are or are not subject to state scrutiny—a change with which much of the Court is clearly uncomfortable[129] and which threatens to vitiate any application of the *Katz* test by undermining privacy expectations.

Fortunately, however, the very same conditions that in the past gave rise to expectations of nonidentification—namely limited police resources and limited memories[130]—also constrain the capacity of identificatory data to meaningfully compromise material privacy interests, even absent a warrant requirement. This is because the information available to state actors far outstrips their capacity to idly compromise the privacy interests of arbitrarily chosen citizens. In particular, in order for identificatory data to be of proper inter-

128. *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring); *see also* Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 242–43 (2002) (discussing the implications of the compromise of public anonymity); Note, *In the Face of Danger: Facial Recognition and the Limits of Privacy Law*, 120 HARV. L. REV. 1870, 1873–75 (2007) (same).

129. *See supra* note 78 and accompanying text.

130. *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring).

est to the state, there must be a situation of which law enforcement is already aware that makes it necessary to identify someone.[131]

Implicitly, then, in order to qualify as an identificatory search not mandating a warrant, the information sought must meet a threshold requirement of at least reasonable suspicion,[132] because only in such situations would there be cause to identify individuals subject to ubiquitous surveillance. Identifying an unknown suspect from a surveillance video is a presumptively valid exercise of state power.[133] Identifying the entrants of a gay bar is not.[134] Because of the implicit requirement that identificatory searches be based on reasonable suspicion, it may well be appropriate to constitutionalize the reasonable suspicion standard for identificatory searches into a conduct rule for law enforcement. Such a standard for identificatory searches would seemingly place de minimis limits on legitimate law enforcement activity while curtailing potential abuses of the identificatory exception (such as observing and identifying all entrants of a mosque or gay bar absent reasonable suspicion[135]). Indeed the National Security Agency's (NSA) phone-metadata collection program already implements precisely such a "reasonable

131. *See, e.g.*, *supra* note 96; *see also* Campbell, *supra* note 104 (describing Los Angeles police's use of already-logged license plate data to correlate the movements of a suspected murderer in the wake of the crime).

132. This standard was first articulated in *Terry v. Ohio*, 392 U.S. 1, 27 (1968), as a limiting principle upon police authority to stop individuals in public suspected of criminal activity who had not engaged in conduct rising to the level of probable cause.

133. *See, e.g.*, Slobogin, *supra* note 128, at 236, (collecting cases and noting, "[A]ll courts that have considered application of the Fourth Amendment to cameras aimed at public streets or other areas frequented by a large number of people have declared that such surveillance is not a search, on the ground that any expectation of privacy one might have in these areas is unreasonable."); *see also supra* Introduction (discussing FBI release of images of the Boston Marathon bombers as a result of sifting through mountains of photographic and videographic evidence).

134. *See* Rehnquist, *supra* note 122, at 9 (discussing use of police car to create list of patrons of a bar during known hours and arguing that there would be a "justified uneasiness" with the arrangement as a result of "a sense that this ought not to be a governmental function").

135. The New York Police Department's recent monitoring of mosques and Muslim student groups, for instance, prompted a resounding backlash at its broad and suspicionless character despite assertions by public officials of its nominal legality. Michael Powell, *Police Monitoring and a Climate of Fear*, N.Y. TIMES, Feb. 28, 2012, at A17 (quoting then-Newark mayor Cory Booker describing the NYPD's program as a "nadir" of law enforcement respect for rights).

suspicion" standard prior to allowing queries, in the interest of limiting idle privacy compromise.[136]

To the extent that reasonable suspicion itself represents a limiting principle on the otherwise near-plenary police power to stop persons in public,[137] the reasonable suspicion standard for identification fulfills a similar role. It allows for a quick review of footage to verify or discredit a report of a hit-and-run or an anonymous tip of a drug deal without representing so much discretion as to vitiate the concerns of the Sotomayor and Alito *Jones* opinions.

C. Principle Three: Constitutionality of Data Gathering Without Human Involvement under the Human Observation Test

Under the Human Observation test the principle that privacy breach turns not on data collection but on data access has the corollary that, ex ante, all information gathering of data within the public domain is constitutional.[138] No constitutional protections inure to the gathering of data from public space under the Human Observation test.[139] Mere gathering is insufficient to violate a *Katz* reasonable expectation,[140] and as such has no attendant warrant requirement. Rather, because the privacy violation attaches to data access—that is, at the point of human involvement—so too does the warrant requirement.

136. Orin Kerr, *Why Does a* Terry *Standard Apply to Querying the NSA Call Records Database?*, VOLOKH CONSPIRACY (June 7, 2013, 12:11 PM), http://www.volokh.com/2013/06/07/why-does-a-terry-standard-apply-to-querying-the-nsa-call-records-database/; *see also* ACLU v. Clapper, 959 F. Supp. 2d 724, 734 (S.D.N.Y. 2013) (discussing the "reasonable articulable suspicion" requirement for NSA metadata database queries, and noting that "[t]he 'reasonable articulable suspicion' requirement ensures an 'ordered and controlled' query and prevents general data browsing").

137. *Terry*, 392 U.S. at 27.

138. Law enforcement surveillance of *private* space is generally beyond the scope of this Note, but a combination of the Fifth Amendment's Takings Clause (as a limiting principle on the use of private property for government surveillance infrastructure) and *Kyllo*'s stringent limitation on the surveillance of the home (concomitant with the Fourth Amendment guarantee of security in "houses") may be taken to provide a basic set of limitations on how far such intrusions could extend. U.S. CONST. amends. IV, V; Kyllo v. United States, 533 U.S. 27, 40 (2001).

139. Specifically because such protection would be overbroad and unnecessarily conflict with law enforcement prerogatives. *See generally* Slobogin, *supra* note 128, at 237 (noting that courts generally find public surveillance compatible with existing Fourth Amendment doctrine).

140. *See* Slobogin, *supra* note 128, at 236; *supra* Part II.C.

IV.
THE BENEFITS OF THE HUMAN OBSERVATION TEST AS A WARRANT GRAVAMEN

A. Technological Progress: Not Putting the Genie Back in the Bottle

One of the foremost benefits of viewing privacy through the lens of a breach/nonbreach binary determined by human observation—rather than solely through an analysis of whether or not a particular mode of information gathering or amount of gathered information is a search—is purely pragmatic. A constitutional definition of "search" that accounts for the privacy compromise potential of collative searches (or "mosaic searches," to use Kerr's terminology)[141]—searches based on the mass aggregation or mining of nominally public but heretofore practically unexamined data—is attractive in part precisely because, as Kerr notes, five of the current nine Justices have already adverted to the idea that there is room for such a notion in our constitutional jurisprudence[142] In practical terms, collative searches enabled by ubiquitous surveillance are likely to find themselves the subject of constitutional scrutiny sooner or later, and thus invite the definition of a legal framework of search that accommodates them.[143]

Nevertheless it is clear that such a framework cannot be generated ex nihilo without any sensitivity to its impact on current infrastructure. In short any attempt to put "mosaic searches" under the Fourth Amendment's purview or to place limitations on ubiquitous surveillance must be sensitive to the simple fact that surveillance cameras are not going away.

As a purely practical matter the removal of surveillance devices already in place[144] is so remote a possibility that any limitation on public data collection that precludes their use is essentially dead on arrival. Courts are likely to be hesitant to institute any order that

141. Kerr, *supra* note 50, at 313.

142. *See supra* note 78.

143. *See* Kerr, *supra* note 50, at 326 ("[F]ive justices wrote or joined opinions that did touch on the mosaic theory. Their opinions are somewhat cryptic, but they suggest that a majority of the Court is ready to embrace some form of the D.C. Circuit's mosaic theory.").

144. The use of "surveillance devices" here refers both to devices run by municipal law enforcement and to those devices installed by third parties (such as store security cameras) and thus usable against a criminal defendant without a warrant under the third-party doctrine. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 743–44 (1979) ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.").

would, for example, scrap the 3000 cameras currently deployed in Lower Manhattan.[145]

Nor would a constitutional theory of ubiquitous surveillance that mandated "putting the genie back in the bottle" (i.e., limiting the use and further deployment of surveillance infrastructure despite a technological trajectory enabling cheaper and more comprehensive surveillance technologies[146]) obviously inure to the benefit of the public in a normative sense. Public surveillance cameras in urban areas routinely prove their worth to law enforcement, whether clarifying the circumstances under which officers discharged their weapons at a man who had recently shot a former coworker at the Empire State Building,[147] or else providing a glimpse, albeit blurry, of the perpetrator of a recent brutal rape in Central Park.[148] The latter circumstance is particularly valuable both with respect to the general interest in efficient law enforcement and especially to any innocent potential defendants who would otherwise find themselves facing accusations based on evidence such as eyewitness testimony. Eyewitness testimony as an evidentiary source has come under increasing scrutiny and criticism, yet it is extremely difficult to refute absent either an objective evidentiary record or a countervailing (and potentially equally unreliable) witness narrative.[149]

Inasmuch as surveillance infrastructure already has and continues to proliferate,[150] the United States has incurred and continues to incur a form of reliance interest on such proliferation being con-

145. Editorial, *Surveillance Cameras a Tool for Deterrence*, BOS. GLOBE (Apr. 20, 2013), http://www.bostonglobe.com/opinion/2013/04/19/surveillance-cameras-are-lot-less-scary-than-bombs/WzCUILoS2N5ralmclr3QRN/story.html.

146. *See, e.g.*, *supra* notes 58 and 65 and accompanying text.

147. Barron, *supra* note 12.

148. Wendy Ruderman & Andy Newman, *Woman, 73, Is Raped in Central Park*, N.Y. TIMES, Sept. 13, 2012, at A24. The rapist was later identified and apprehended. Wendy Ruderman & Nate Schweber, *Drifter Known for Menace Is Charged with Raping Woman, 73, in Central Park*, N.Y. TIMES (Sep. 14, 2012), at A20.

149. *See, e.g.*, Derek Simmonsen, *Teach Your Jurors Well: Using Jury Instructions to Educate Jurors about Factors Affecting the Accuracy of Eyewitness Testimony*, 70 MD. L. REV. 1044, 1044 (2011) ("[A]ccording to one recent study, erroneous eyewitness testimony is the single largest cause of wrongful convictions in capital cases."); Wayne T. Westling, *The Case for Expert Witness Assistance to the Jury in Eyewitness Identification Cases*, 71 OR. L. REV. 93, 95 (1992) (discussing problems with eyewitness identification and noting courts' attention to the issue, noting that "[c]ommentators from both the legal community and the scientific community agree that eyewitness identification is unreliable"). *See generally supra* note 24.

150. Most notably U.S. law enforcement has dramatically increased its acquisition and deployment of domestic surveillance drones. *Supra* note 13.

stitutionally sound. Because the "human observation" criterion at most requires procedural alteration without actually affecting the deployment of physical infrastructure, courts may invoke it to maintain oversight of law enforcement without seriously disrupting this reliance interest. Since the magnitude of this reliance interest is by now so great that the judiciary will not realistically be in a position to ignore it,[151] the Human Observation test meets the threshold requirement of respecting the reliance interest of surveillance infrastructure in a way that more aggressive attempts to rein in surveillance proliferation may not.

B. Clarity and Justiciability

The main thrust of Orin Kerr's objections to the "mosaic search" concept advanced in the Sotomayor and Alito opinions of *Jones* is that it is such a fundamental divorce from the previously dominant paradigm of Fourth Amendment searches that an extremely large host of novel questions would need to be answered by courts before any coherent notion of "mosaic search" (and the attendant regulation of law enforcement) could coalesce.[152] Making human observation a Fourth Amendment gravamen is valuable not just because it represents an attractive alignment between the philosophical notion of privacy and the legal concept thereof,[153] but also because it renders many of these legal questions either moot or else relatively easily answered in practice.

An obvious critique of a mosaic theory of the Fourth Amendment[154] is that even if the power of collating data "exposed to the

151. For instance, even a small number of police drones for a single department represents an outlay of thousands to tens of thousands of dollars. *See, e.g.*, Alison Veshkin, *Police Drones Aimed at Berkeley's Skies Rankle Privacy Activists*, BLOOMBERG (Jan. 13, 2015), http://www.bloomberg.com/news/articles/2015-01-13/police-drones-aimed-at-berkeley-s-skies-rankle-privacy-activists ("Alameda County bought two unmanned aircraft weighing about 4 pounds (1.81 kilograms) for about $97,000 last year.").

152. Kerr, *supra* note 50, at 353 ([T]he mosaic theory represents a Pandora's Box that courts should leave closed. The theory raises so many novel and difficult questions that courts would struggle to provide reasonably coherent answers. By the time courts worked through answers for any one technology, the technology would likely be long obsolete.").

153. *See* Tokson, *supra* note 110, at 616 (arguing that "our concept of a loss of privacy [including in the legal sense] is inextricably bound up in the idea of a human observer").

154. The "mosaic theory" of the Fourth Amendment refers to a Fourth Amendment paradigm that recognizes the privacy-compromising power of collated information. For a discussion of collated information's capacity to compromise privacy in a manner analogous to Kerr's "mosaic search" concept, see *Riley v.*

public"[155] offends both the lay understanding of privacy and the sensibilities of the Justices, this hardly makes it clear precisely *when* privacy is threatened by a collative search:

> The first initial grouping question is the most obvious: how long must the tool be used before the relevant mosaic is created? In *Jones*, the GPS device was installed for twenty-eight days. Justice Alito stated that this was "surely" long enough to create a mosaic. But he provided no reason why, and he recognized that "other cases may present more difficult questions." If twenty-eight days is too far, how about fourteen days? Or 3.6 days? Where is the line?[156]

Law enforcement and intelligence officers can hardly be expected to make do with imprecise balancing tests when determining whether or not to get a warrant. Society would generally prefer that police officers not routinely grapple with extracting an essentially binary answer (warrant required/no warrant required) from the semantic morass of "reasonable expectations of privacy."[157] Indeed an examination of seminal post-*Katz* Supreme Court decisions reveals that typically the constitutionality of specific law enforcement *techniques* is at issue rather than, for example, a particular school of interpretation of *Katz*.[158] Any theory of "mosaic search" must therefore make it clear from the outset when and whether a warrant is required for any particular act of law enforcement. Kerr objects to "mosaic search" theory precisely because he believes that a collation-oriented conception of a search fails to answer the question of "exactly when is this activity enough to mandate a warrant?"[159]

The Human Observation test, however, answers this question quite straightforwardly.[160] When do warrant protections attach?

California, 134 S. Ct. 2473, 2489–90 (2014) ("The storage capacity of cell phones has several interrelated consequences for privacy. First, a cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record."). *See also* Kerr, *supra* note 50 and accompanying text.

155. *See supra* Part I.B.

156. Kerr, *supra* note 50, at 333; *see also* United States v. Jones, 132 S. Ct. 945, 954 (2012) (highlighting similar duration-based line drawing questions invited by Justice Alito's concurrence in judgment).

157. Kerr, *supra* note 50, at 315–16 (discussing courts' traditional use of act-based formalism in evaluating whether or not a Fourth Amendment search has occurred).

158. *Id.*

159. *Id.* at 333.

160. At least with respect to information gained by *passive* surveillance. *See supra* Part II.B.

They attach as soon as law enforcement has a specific, identified suspect and wishes to learn about his or her comings and goings beyond the information required to identify the suspect and/or the information which initially gives rise to reasonable suspicion.[161] Indeed arguably the chief virtue of the Human Observation test is that it entwines the act of privacy breach (and its attendant Fourth Amendment warrant requirement) with a fairly straightforward conduct rule. Once "John Doe" is actively sought by a human being, warrant protections attach, and the parade of horrors alluded to by Kerr, including a constant need for judicial factor-balancing, is effectively cabined.

Ironically despite his argument against judicial recognition of "mosaic search" as an independent Fourth Amendment gravamen,[162] Kerr himself has advocated the use of an approach akin to the Human Observation test proposed in this Note for determining when a search occurs during the access of computerized data. Specifically Kerr has advocated what he calls an "exposure-based approach" in this context for a number of reasons,[163] including the ease of administering such a test.[164] As this Note argues, however, Kerr's test for when a search occurs vis-à-vis computer data is readily extensible to any search that uses passive technological means for surveillance. By treating human observation as a condition precedent to a privacy breach, the concerns judges have expressed about "mosaic searches" can be incorporated into Fourth Amendment doctrine in one fell swoop without meaningfully upsetting precedents pertaining to more traditional forms of search. The Human Observer test thus preserves both conceptual clarity and easy justiciability.

C. Evidentiary Availability

The appeal of allowing unfettered data gathering and of placing restrictions on the use of surveillance infrastructure only at the

161. *See supra* Part II.

162. Kerr, *supra* note 50, at 353 (arguing that "mosaic search" creates too many complicated judicial questions and that a purely sequential approach to search theory is superior). Note that the "human observer" criterion is in fact compatible with Kerr's argument in favor of maintaining a sequential approach to search doctrine, with the act triggering the warrant requirement being the moment of human engagement.

163. Kerr, *supra* note 110, at 551 (explaining that under his "exposure-based approach," "a search occurs when information from or about the data is exposed to possible human observation, such as when it appears on a screen, rather than when it is copied by the hard drive or process by the computer").

164. *Id.* at 552.

time of human access is that it alleviates a perennial problem of both law enforcement and of trial practice: the absence, even in principle, of crucial information. As objective records proliferate, accessible through the use of warrants, the problems of witness unreliability—faulty perception,[165] faulty recall, unavailability, and perjury—lessen.[166] Particularly as evidence mounts about the unreliability of eyewitness testimony, alternative objective evidentiary methods become more attractive, lessening the need for adversary gamesmanship to determine "what actually happened."[167] Crucially, the ubiquitous availability of surveillance information is as much a boon to the innocent as it is injurious to the guilty. Objective evidence pointing to the actual perpetrators of crimes lessens the likelihood of wrongful imprisonment arising from reliance on fallible human perception and recall.[168] Accordingly a scheme which preserves constitutional Fourth Amendment minima but maximizes the nominal availability of data will generally promote the administration of both civil and criminal justice through provision of objective evidentiary records.

V.
OVERSIGHT AND PRACTICAL CONSTRAINTS ON ABUSE

Any increase in governmental power evinces the specter of abuse. Although the benefits to law enforcement of the use of surveillance infrastructure are self-evident, the idea that ubiquitous surveillance represents a threat to free society has had adherents from George Orwell in 1949[169] to Justice Sotomayor in 2012.[170]

165. *See generally* Westling, *supra* note 149; Simmonsen, *supra* note 149.

166. *See, e.g.*, United States v. White, 401 U.S. 745, 787 (1971) (Harlan, J., dissenting) ("The argument . . . that it is irrelevant whether secrets are revealed by the mere tattletale or the transistor, ignores the differences occasioned by third-party monitoring and recording which insures full and accurate disclosure of all that is said, free of the possibility of error and oversight that inheres in human reporting.").

167. *See generally* Westling, *supra* note 149; Simmonsen, *supra* note 149.

168. *Id.*

169. *See generally* ORWELL, *supra* note 58.

170. United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)) ("I would also consider the appropriateness of entrusting to the Executive, in the absence of any oversight from a coordinate branch, a tool so amenable to misuse, especially in light of the Fourth Amendment's goal to curb arbitrary exercises of police power to and prevent 'a too permeating police surveillance.'").

It is therefore appropriate to highlight the relatively attenuated prospects for one of the most obvious concerns evinced by allowing unfettered data gathering: abuse. There are three basic constraints on the capacity of law enforcement to use ubiquitous surveillance technology in inappropriate ways (that is, exceeding their authorization as agents of law enforcement): (1) practical incapacity, (2) audit logging, and (3) use of surveillance infrastructure to monitor law enforcement actions.

This Note does not argue that there is a de minimis or inconsequential risk of abuse by governmental authorities—quite the contrary, it acknowledges that there is a litany of both potential and realized risks posed by expansive governmental surveillance powers. Rather the claim is that, as a normative matter, the risks to individual liberties posed by a centralized infrastructure subject to judicial and political oversight are likely to be less than those posed by the criminal activities such infrastructure is designed to prevent and punish.

A. Practical Incapacity

"Practical incapacity" refers to the basic idea that, in a country with finite law enforcement officers, already-backlogged investigations, and millions of citizens, the police lack either the capacity or indeed the will to routinely audit the comings and goings of average citizens. Consider what it would mean for the police to meaningfully review, over any nontrivial period of time, the comings and goings of the typical reader of this Note. The reader would have to be: (1) known to the police; (2) of more than passing interest to the reviewing officer—in particular, of greater interest than all of the other citizens of pertinent locality; and (3) more important to the reviewing officer than the actual performance of said officer's primary job, which presumably does not include monitoring the activities of members of the legal profession not suspected of any offense.

These basic criteria are hardly impossible to meet—consider the ex-romantic partner of a police officer, or a prominent or controversial political candidate—but together they constitute a high enough bar that the risk of any living, breathing government agent taking an interest in an arbitrary person's comings and goings is, at the least, somewhat remote. In essence this argument reiterates the basic paradox of "Big Data": the larger the haystack of data, the more time, effort, and expense are required to actually use it in

anything but an indexed and targeted manner.[171] Federal Rule of Evidence 1006 allows the introduction in court of summaries of long documents precisely due to the recognition that search costs are significant when the amount of raw data is large.[172] The greatest protection to the typical citizen against even the determinedly abusive practice of law enforcement is that there are, simply put, too many genuine crimes to investigate to make the typical person's daily outings very interesting.[173] In other words not only does the Human Observation test place restrictions on when law enforcement officers may look, but the very context that necessitates its use suggests that for most individuals there is very little incentive to look in the first place.

B. Audit Logging

Nevertheless the fear of abuse is unquestionably one of the central drivers behind the warrant requirement and its attendant demand that a neutral magistrate sign off on certain police invasions of privacy.[174] Nor has the Constitution recognized a diminished Fourth Amendment right with respect to public figures (notwithstanding the presumably diminished expectations of privacy they have vis-à-vis *private* surveillance such as tabloids or the press),[175] suggesting further limitation on the idea that the large pool of mundane potential surveillance targets reduces the risk of

171. Bruce Schneier, Op-Ed., *Why FBI and CIA Didn't Connect the Dots*, CNN (May 2, 2013, 3:37 PM), http://edition.cnn.com/2013/05/02/opinion/schneier-boston-bombing/index.html (discussing problems caused by finding patterns ex ante in large amounts of data without organizing principles).

172. *See* FED. R. EVID. 1006; FED. R. EVID. 1006 advisory committee's note ("The admission of summaries of voluminous books, records, or documents offers the only practicable means of making their contents available to judge and jury.").

173. The total uniformed strength of the New York Police Department is approximately 34,500. *Frequently Asked Questions*, NYPD, http://www.nyc.gov/html/nypd/html/faq/faq_police.shtml#1 (last visited Feb. 16, 2015). The number of reported crimes limited solely to the top "seven major felony offenses" in 2014 was 111,335. *Historical New York City Crime Data*, NYPD, http://www.nyc.gov/html/nypd/html/analysis_and_planning/historical_nyc_crime_data.shtml (last visited Apr. 6, 2015). Combining all criminal complaints there were 528,335 felonies and misdemeanors in 2013 and 61,037 violations. *Id.*

174. *See* U.S. CONST. amend. IV ("[N]o 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.").

175. Sherry F. Colb, *What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 STAN. L. REV. 119, 176 (2002) ("Though there is nothing in Fourth Amendment law to distinguish [well-known public figures] from someone like Knotts, the First Amendment has a vocabulary to accommodate the distinction.").

surveillance misuse. So long as there are figures of public interest, there are risks of abuse.

Fortunately, however, the same computerized infrastructure that enables information analysis from a desktop can also provide a log of activities that can be used to track law enforcement use patterns for abuse. Indeed such a log is more easily reviewed than many physically undertaken police surveillance activities.[176] Audit logging allows for internal, centralized checks on who is doing what—arguably a much easier task than, for instance, keeping tabs on officers in the field attaching GPS trackers to cars under the auspices of expired warrants.[177]

In a striking recent example, press coverage of compliance lapses at the NSA, revealed in documents leaked by Edward Snowden, highlights the thousands of such lapses that occur yearly.[178] Many such lapses are apparently due to targets of foreign surveillance wiretaps subsequently entering the United States, where such wiretaps require a warrant.[179] Although an NSA official alleged that these thousands of incidents appear less severe when viewed as an overall percentage of NSA intelligence queries,[180] what is perhaps most striking about the compliance lapse information is that it is the result of an internal audit, one conducted extensively with the use of automated audit tools.[181] Even as Snowden's disclosures exposed the NSA's program to unexpected public scrutiny,

176. *See* HARRIS, *supra* note 96, at 256 (discussing John Poindexter's proposal for the proposed Total Information Awareness domestic intelligence system's ability to prevent abuse despite its vast capacity: "Simple, Poindexter declared. TIA would be used to monitor the people using it—watching the watchers, logging all abuses").

177. *See* United States v. Jones, 132 S. Ct. 945, 946–47 (2012) (describing use of a GPS tracker on suspect's car with an expired warrant).

178. Barton Gellman, *NSA Broke Privacy Rules Thousands of Times Per Year, Audit Finds*, WASH. POST (Aug. 15, 2013), http://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html.

179. Charlie Savage, *N.S.A. Often Broke Rules on Privacy, Audit Shows*, N.Y. TIMES, Aug. 16, 2013, at A12 ("The largest number of episodes—1,904—appeared to be 'roamers,' in which a foreigner whose cellphone was being wiretapped without a warrant came to the United States, where individual warrants are required.").

180. *Id.* (quoting an anonymous senior NSA official speaking with White House permission).

181. *Id.*; *see also* NSA, SIGNALS INTELLIGENCE DIV., INTELLIGENCE OVERSIGHT QUARTERLY REPORT—FIRST QUARTER CALENDAR YEAR 2012 (1 JANUARY–31 MARCH 2012)—EXECUTIVE SUMMARY 8 (2012), *available at* http://apps.washingtonpost.com/g/page/national/nsa-report-on-privacy-violations-in-the-first-quarter-of-2012/395/ (noting that automated alerts were by far the largest source of reported noncompliance incidents).

the very existence of the data scrutinized testifies to the practicality of coupling ubiquitous surveillance practices to equally comprehensive oversight systems.

In other words there is little reason to believe that auditing to ensure compliance with constitutional use restrictions (and attendant discipline for flouting such restrictions) is incompatible with or inimical to massive data gathering efforts, even for a relatively opaque organization such as the NSA. Thus, a fortiori, expecting and mandating auditing should not be an implausible requirement for law enforcement agencies that act under more direct oversight and with fewer clandestine procedures.

C. Quis Custodiet? Watching the Watchers

Crucially, knowledge that law enforcement officers themselves are subject to the same ubiquitous surveillance infrastructure used to deter and prosecute criminal conduct has tremendous potential to remedy police abuses that presently occur. Such has been the experience of the Rialto, California Police Department, where uniform recording of police-civilian interactions resulted in a year-on-year reduction in complaints to the department of 88%,[182] with the program winning plaudits from both police officers who were able to easily deal with meritless abuse claims[183] and from civil libertarians in the ACLU supporting the monitoring of police activities.[184]

Hearkening back to the idea that ubiquitous surveillance frees courts from the evidentiary pitfalls of witness fallibility and credibility in favor of reliance on objective evidence, even potential targets of law enforcement may find themselves aided by an infrastructure that makes police abuses available in court. For instance, the availa-

182. Randall Stross, *Wearing a Badge, and a Video Camera*, N.Y. TIMES, Apr. 7, 2013, at B4.

183. *Id.* (citing Rialto police chief William Farrar relating anecdotes involving citizen complaints being abandoned in the wake of station officers showing video of the incidents to would-be complainants); Neill Franklin, Op-Ed., *Body Cameras Could Restore Trust in Police*, N.Y. TIMES (Oct. 22, 2013), http://www.nytimes.com/roomfordebate/2013/10/22/should-police-wear-cameras/body-cameras-could-restore-trust-in-police (advocating police cameras, written by thirty-four-year veteran of Maryland police forces and former commander of training, both to protect police from misconduct accusation as well as to improve force discipline and to negate the "blue wall of silence" in which law enforcement institutions refuse to admit to any allegations of misconduct).

184. Stross, *supra* note 182 (citing ACLU analyst Jay Stanley's support for the program so long as it maintains use and retention limits, and quoting him as stating that "[t]he technology really has the potential to level the playing field in any kind of controversy or allegation of abuse").

bility of an objective record no longer forces plaintiffs in excessive force cases to put their own word—potentially suspect in the case of those with criminal histories subject to impeachment[185]—against that of a police officer.[186] To the extent that the Human Observation test encourages rather than hinders the proliferation of surveillance infrastructure, then, it not only aids law enforcement but also the civilians subject to law enforcement's conduct.

D. The Normative Tradeoff: Abuse Risk Versus Use Utility

Ultimately the risk of abuse of ubiquitous surveillance infrastructure, even with use restrictions in place, cannot be eliminated (though it can be mitigated). Rather than suggest that the unfettered information gathering allowable under a Human Observation model of Fourth Amendment search is costless, this Note submits that the mitigations available to limit such costs highlight the fundamental normative tradeoff of surveillance in a manner that suggests that its benefits to the typical citizen are greater than its risks. A centralized monitoring infrastructure (subject, in turn, to comparatively easy physical and electronic oversight) with internal audit logging, combined with surveillance methods that record law enforcement activity as well as that of ordinary citizens, presents less material risk of harm to the typical citizen than does terrorism at a marathon—or more likely harms such as mugging, burglary, or assault. This is the normative tradeoff—unsolved or harder-to-solve crimes versus a group of government agents potentially engaging in idle privacy compromise—invited by a use-restriction model of surveillance that places the warrant requirement at the time of exposure to human observation rather than placing ex ante procedural limits on data gathering. This Note submits that in general the capacity to monitor and redress any harms will be more effective when press, political, and electoral pressures can be brought to bear on centralized government bureaucracy than when faced with the doings of innumerable private criminal actors.

185. *See* FED. R. EVID. 609.

186. Stross, *supra* note 182 (citing ACLU analyst Jay Stanley's approval of the program's potential to reduce the need for credibility determinations, and quoting him as saying that "there were so many situations where it was 'he said, she said,' and juries tend to believe police officers over accused criminals").

VI.
LESSONS FROM THE NATIONAL SECURITY INTELLIGENCE EXPERIENCE: USE RESTRICTIONS AS A PRACTICAL COMPROMISE ALREADY IN USE

Although this Note is primarily interested in the ubiquitous surveillance of public space, the general topic of ubiquitous surveillance has in recent months been most strongly identified in public discourse with the methods employed by the NSA to record and access bulk metadata about the phone interactions of millions of American citizens.[187] As a preliminary matter the national security apparatus is by design significantly less subject to public oversight than standard law enforcement.[188] Intelligence gathering activities requiring court authorization are often conducted after closed proceedings in the Foreign Intelligence Surveillance Court (FISC), a specially convened tribunal staffed by district court judges who are assigned to it on a temporary basis in addition to their main judicial appointments.[189]

The same basic normative tradeoff of the Human Observation test is presented in both the law enforcement and intelligence contexts: in both instances the need to oversee a centralized and well-known government authority in order to prevent subversion of an access-restriction warrant regime must be balanced against the risk of hostile third parties (i.e., criminals in the law enforcement case, terrorists and hostile states in the intelligence context) causing harm to citizens.[190] However, the risk of abuse of ubiquitous surveillance infrastructure is likely higher (due to laxer oversight)[191] and the risk of harm in its absence lesser (due to the statistical rarity of

187. Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN (June 6, 2013, 6:05 PM), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order; *see also* Barton Gellman, *Edward Snowden: 'I Already Won*,*'* WASH. POST, Dec. 24, 2013, at A1 (discussing NSA information leaked by Edward Snowden). *See generally* Dustin Volz, *Everything We Learned from Edward Snowden in 2013*, NAT'L J. (Dec. 31, 2013), http://www.nationaljournal.com/defense/everything-we-learned-from-edward-snowden-in-2013-20131231 (providing an overview and timeline of the various NSA surveillance intelligence disclosures made public by Edward Snowden).

188. *See* ACLU v. Clapper, 959 F. Supp. 2d 724, 731 (S.D.N.Y. 2013) (discussing Foreign Intelligence Surveillance Court used in warrant issuance and judicial oversight of NSA intelligence activities).

189. *See id.* at 730–35 (discussing of the history of FISA and the FISC in the NSA surveillance context).

190. *See supra* Part III.D.

191. *See supra* note 178 and accompanying text.

harms like terrorist attacks, dramatic though they may be)[192] in the intelligence context.[193] This dichotomy suggests that the normative tradeoffs at stake may differ even if the philosophical underpinnings of the access/gathering distinction remain sound.[194]

Yet despite having arguably the weaker case for adoption of the model, the American national security apparatus has in fact already largely oriented itself towards an access-restriction plus ubiquitous data-gathering paradigm, having longer faced the privacy concerns evinced by a vast surveillance infrastructure.[195] In fact the national security apparatus' use-restriction paradigm appears to be hewing even closer to the "if human access, then warrant" position advocated by this Note in the wake of the intelligence leaks by Edward Snowden and the resultant political furor.[196] Moreover in one of the two recent court cases to consider the general constitutionality

192. For example, the terrorist attacks of September 11th, 2001 resulted in casualties of 2977 people, excluding the hijackers. *September 11th Fast Facts*, CNN (Sept. 8, 2014, 12:54 PM), http://www.cnn.com/2013/07/27/us/september-11-anniversary-fast-facts/. The United States counted 16,037 murders and nonnegligent manslaughters (excluding the September 11th attacks) that year alone; between 2001 and 2012 there were 192,193 murder and nonnegligent manslaughters in the United States. U.S. Dep't of Justice, FBI, *Uniform Crime Reporting Statistics*, http://www.ucrdatatool.gov/Search/Crime/State/TrendsInOneVar.cfm (select "United States—Total"; then select "Murder and nonnegligent manslaughter"; then select years "2001" to "2012"; then select "Get Table") (last accessed Feb. 6, 2015).

193. Klayman v. Obama, 957 F. Supp. 2d 1, 18 n.23 (D.D.C. 2013) (noting serious compliance problems with FISC supervision of the NSA). Two conflicting district court opinions recently reached starkly different conclusion as to the constitutionality of the NSA's surveillance program. *Compare* ACLU v. Clapper, 959 F. Supp. 2d 724, 752 (S.D.N.Y. 2013) (finding the program to be constitutional and within Fourth Amendment bounds, although rejecting the idea that querying is a search and describing the ACLU's reliance on the concurring *Jones* opinions as "misplaced"), *with Klayman*, 957 F. Supp. 2d at 41 (finding, in preliminary injunction context, that NSA phone record metadata collection is likely unconstitutional under the Fourth Amendment).

194. *Cf. supra* note 193 (conflicting constitutionality decisions reached by recent district courts to consider program's constitutionality).

195. Kerr, *supra* note 136 ("The NSA call records program appears to be that idea on steroids: Collect everything, and then control access to the database created. But I'm left puzzled as to what the legal basis is for what appears to be happening. Where are they getting the *Terry* standard here?").

196. Ellen Nakashima & Greg Miller, *Obama Calls for Significant Changes in Collection of Phone Records of U.S. Citizens*, WASH. POST (Jan. 17, 2014), http://www.washingtonpost.com/politics/in-speech-obama-to-call-for-restructuring-of-nsas-surveillance-program/2014/01/17/e9d5a8ba-7f6e-11e3-95c6-0a7aa80874bc_story.html ("Obama directed that from now on, the government must obtain a court order for each phone number it wants to query in its database of records.").

of the program, such controls were cited as evidence of the effectiveness of the program and signifiers of its constitutionality.[197]

The two district courts that have considered the constitutionality of the NSA metadata-collection program have reached starkly opposite conclusions, in part because of wildly varying conceptions of whether or not existing Fourth Amendment jurisprudence can be adapted to new technologies.[198] Both decisions have since been appealed and argued in their respective circuits but are awaiting disposition at the time of this writing,[199] and so this Note will concern itself only with their reasoning at the district court level.

ACLU v. Clapper, decided in the Southern District of New York, found the NSA metadata collection program constitutional.[200] It relied largely on Supreme Court precedent, in particular *Smith v. Maryland*,[201] a case dealing with similar telephony metadata that permitted the automated recording of numbers dialed by a telephone using a pen register.[202] *Clapper* in essence declined to grant constitutional significance to the scale of ubiquitous surveillance records in the presence of otherwise-applicable Supreme Court precedent.[203]

Conversely in *Klayman v. Obama* the D.C. District Court granted a preliminary injunction based on the likely unconstitu-

197. *Clapper*, 959 F. Supp. 2d at 750 (rejecting ACLU's "mosaic" argument that NSA program breaches Fourth Amendment privacy expectations in part based on governmental data use restrictions). *But cf. Klayman*, 957 F. Supp. 2d at 32, 39 n.62 (finding use restrictions not sufficient to meet Fourth Amendment strictures and stating, "I believe that bulk telephony metadata collection and analysis almost certainly does violate a reasonable expectation of privacy.").

198. *Compare Clapper*, 959 F. Supp. 2d at 752 (finding the program to be constitutional and within Fourth Amendment bounds), *with Klayman*, 957 F. Supp. 2d at 41 (finding, in preliminary injunction context, that NSA phone record metadata collection is likely unconstitutional under the Fourth Amendment).

199. *See* Notice of Appeal, *Clapper*, 959 F. Supp. 2d 724 (S.D.N.Y. 2013) (No. 13 Civ. 03994); Notice of Appeal, *Klayman*, 957 F. Supp. 2d 1 (D.D.C. 2013) (Nos. 13 Civ. 00851 & 13 Civ. 0081).

200. 959 F Supp. 2d at 754.

201. 442 U.S. 735 (1979).

202. *Clapper*, 959 F. Supp. 2d at 752 ("Some ponder the ubiquity of cellular telephones and how subscribers' relationships with their telephones have evolved since *Smith*. While people may 'have an entirely different relationship with telephones than they did thirty-four years ago,' this Court observes that their relationship with their telecommunications providers has not changed and is just as frustrating.").

203. *Id.* ("The collection of breathtaking amounts of information unprotected by the Fourth Amendment does not transform that sweep into a Fourth Amendment search.").

tionality of the program.[204] The holding rested largely on the grounds that technological advancement had so outstripped existing doctrine that new constitutional constraints were warranted:

> When do present-day circumstances—the evolutions in the Government's surveillance capabilities, citizens' phone habits, and the relationship between the NSA and telecom companies—become so thoroughly unlike those considered by the Supreme Court thirty-four years ago that a precedent like *Smith* simply does not apply? The answer, unfortunately for the Government, is now.[205]

In particular, *Klayman* distinguished the collection of phone records for use in an ongoing, active investigation from the capacity for retrospective search enabled by the maintenance of a large volume of such records.[206] Thus the *Klayman* opinion correctly parsed what this Note argues to be the key distinction between the Fourth Amendment jurisprudence of previous technological eras and that of the present one: the novelty of retrospective search of comprehensive records. *Klayman* further intimates, but does not hold, that the absence of individualized judicial authorization for records searches under the NSA program contributed to the finding of unconstitutionality,[207] particularly given the court's skepticism about NSA compliance with internal executive branch authorization protocols.[208]

---

204. *Klayman*, 957 F. Supp. 2d at 43. The court order was stayed pending appeal. *Id.* at 10.

205. *Id.* at 31; *see also supra* Part I.C.

206. *Klayman*, 957 F. Supp. 2d at 32 ("This short-term, forward-looking (as opposed to historical), and highly-limited data collection is what the Supreme Court was assessing in *Smith*. The NSA telephony metadata program, on the other hand, involves the creation and maintenance of a historical database containing *five years'* worth of data. And I might add, there is the very real prospect that the program will go on for as long as America is combatting terrorism, which realistically could be forever!").

207. *Id.* at 37 ("[T]he question . . . is whether people have a reasonable expectation of privacy that is violated when the Government, without any basis whatsoever to suspect them of any wrongdoing, collects and stores for five years their telephony metadata for purposes of subjecting it to high-tech querying and analysis without any case-by-case judicial approval."). The judge in *Klayman* further stated, "I cannot imagine a more 'indiscriminate' and 'arbitrary invasion' than this systematic and high-tech collection and retention of personal data on virtually every single citizen for purposes of querying and analyzing it without prior judicial approval." *Id.* at 42.

208. *See Klayman*, 957 F. Supp. 2d at 18–19 (recounting extensive noncompliance by the NSA with requirements set by the FISC).

Ultimately neither opinion is wholly correct. Although *Clapper* found NSA metadata gathering constitutional—the correct result under the Human Observation test—the opinion rejects the Human Observation test's core tenet that a human query represents a potential Fourth Amendment privacy breach even given the abstract permissibility of comprehensive data gathering.[209] Conversely the *Klayman* opinion considered the advancement of technology to have essentially invalidated relevant precedent due to technological advances that could not have been foreseen by previous Supreme Court majorities[210] and discussed at length the government's system of use restrictions and the perceived shortcomings thereof, including lack of judicial authorization for searches.[211] However, the opinion stopped short of announcing what rules ought to be used in a world in which technological advance outstrips precedent. Crucially, it also elided the distinction between mere *data gathering*, performed by unthinking automatons, and *privacy breach*, conducted by humans observing and working with that data.[212]

Under the Human Observation paradigm the primary emphasis of both the *Klayman* and *Clapper* opinions should be the precise use restrictions in place and the degree of compliance exhibited by the NSA. The analysis, if followed, would result in holdings that essentially enforce a "court order before a query"[213] mandate—such as the one that President Obama himself recently mooted as an in-

209. ACLU v. Clapper, 959 F. Supp. 2d 724, 751 (S.D.N.Y. 2013) ("[T]he Government's subsequent querying of the telephony metadata does not implicate the Fourth Amendment.").

210. *Klayman*, 957 F. Supp. 2d at 33 ("[T]he almost-Orwellian technology that enables the Government to store and analyze the phone metadata of every telephone user in the United States is unlike anything that could have been conceived in 1979.").

211. *Id.* at 18–19, 30 (discussing compliance issues and characterizing the *Katz* inquiry as permitting government retention of "metadata for five years, and then quer[ying], analyz[ing], and investigat[ing] that data without prior judicial approval of the investigative targets").

212. *Id.* at 29 n.39 ("[I]t is irrelevant for Fourth Amendment purposes that the NSA might sometimes use automated analytical software."). Conversely *Clapper* alluded briefly to the notion that individuated searches represent greater privacy compromise than general database-wide ones. *Clapper*, 959 F. Supp. 2d at 750 ("The privacy concerns at stake in *Smith* were far more individualized than those raised by the ACLU. *Smith* involved the investigation of a single crime and the collection of telephone call detail records collected by the telephone company at its central office, examined by the police, and related to the target of their investigation, a person identified previously by law enforcement."); *cf. supra* Part II.C.

213. *See, e.g.*, *supra* Part II. In this instance the requirement of court intervention prior to entering a search query is substantively analogous to the use of a

ternal executive-branch policy[214]—as a prospectively applicable constitutional rule.

Long faced with the need to reconcile the ostensibly conflicting requirements of large-scale intelligence gathering in the interests of national security with the rule of law and legal compliance, a surveillance regulatory regime focused on data access represents the agreed-upon compromise within the executive branch. The Human Observation test aims both to provide constitutional blessing to data gathering under the auspices of such programs[215] and to guide courts exercising oversight of them.

CONCLUSION

Courts have expressed significant discomfort with the adequacy of existing constitutional privacy jurisprudence, given the erosion of background assumptions of generally scarce information by surveillance technology.[216] Most recently five of nine Justices have intimated that, despite the continued vitality of the *Katz* test, a reexamination of Fourth Amendment privacy protections may be warranted in an age of ubiquitous surveillance.[217] Any such constitutional considerations must be sensitive not merely to the obvious benefits to law enforcement and the public at large from increased surveillance infrastructure, but also to municipal reliance interests

search warrant inasmuch as both establish procedures of judicial preauthorization for the conduct of a search. *See infra* note 214.

214. Nakashima & Miller, *supra* note 196. *See generally Klayman*, 957 F. Supp. 2d at 18–19 (citations omitted) (discussing the period in which per-query judicial authorization was the norm with respect to NSA metadata searches as a sanction imposed by the FISC for perceived compliance lapses, and noting that a judge had "ordered the NSA to seek FISC approval on a case-by-case basis before conducting any further queries of the bulk telephony metadata collected pursuant to Section 1861 orders" after "conclud[ing] that he had no confidence that the Government was doing its utmost to comply with the court's order"—an approval procedure that "remained in place from March 2009 to September 2009"). As the *Klayman* citation demonstrates, requiring judicial approval prior to individuated queries is a perfectly practical paradigm for ubiquitous surveillance databases inasmuch as such a scheme was in fact implemented for six months.

215. *See* Kerr, *supra* note 136 (inquiring as to the legal origin of the NSA use-restriction paradigm originating from the FISC, albeit under a reasonable suspicion rather than probable cause standard).

216. *See supra* Parts I.D–F.

217. United States v. Jones, 132 S. Ct. 945 (2012). *See also* Kerr, *supra* note 50, at 326 ("[F]ive justices wrote or joined opinions that did touch on the mosaic theory. Their opinions are somewhat cryptic, but they suggest that a majority of the Court is ready to embrace some form of the D.C. Circuit's mosaic theory.").

in such infrastructure and the need to create an appropriately justiciable standard for any limitations on police conduct.

Establishing at least one parameter of the heretofore nebulous notion of "privacy" protected by *Katz*—that a necessary condition of a breach of privacy is the exposure of information to human observation—suggests that Fourth Amendment warrant protections should apply to data *access* rather than data *gathering*. This serves as a justiciable limiting principle on ubiquitous surveillance that protects *Katz* privacy interests without unduly inhibiting the advantages of surveillance, such as reducing reliance on potentially fallible witness narratives and limiting police misconduct. Since this principle only applies to human review of data passively gathered by machine, it addresses the information-scarcity concerns created by advancing technology while leaving the historical body of Fourth Amendment law largely intact. Courts should encourage the development of a ubiquitous-surveillance Panopticon, but police the boundaries of who is allowed to look in.