MAKING THE MOST OF *UNITED STATES V. JONES* IN A SURVEILLANCE SOCIETY: A STATUTORY IMPLEMENTATION OF MOSAIC THEORY

CHRISTOPHER SLOBOGIN*

I. INTRODUCTION

In the Supreme Court's recent decision in United States v. Jones*, a majority of the Justices appeared to recognize that under some circumstances aggregation of information about an individual through governmental surveillance can amount to a Fourth Amendment search. If adopted by the Court, this notion—sometimes called "mosaic theory"—could bring about a radical change to Fourth Amendment jurisprudence, not just in connection with surveillance of public movements—the issue raised in* Jones*—but also with respect to the government's increasingly pervasive record-mining efforts. One reason the Court might avoid the mosaic theory is the perceived difficulty of implementing it. This article provides, in the guise of a model statute, a means of doing so. More specifically, this article explains how proportionality reasoning and political process theory can provide concrete guidance for the courts and police in connection with physical and data surveillance.*

In *United States v. Jones*,[1] the Supreme Court took a giant step into the modern age. Ignoring the insinuation of its own precedent, the entire Court, albeit in three separate opinions, signaled that technological tracking of a car can be a search under the Fourth Amendment.[2] Even more importantly, all three opinions in *Jones*

* Milton Underwood Professor of Law, Vanderbilt University Law School. The author would like to thank participants in workshops at Vanderbilt Law School and at the Privacy Law Scholars' Conference, June 8, 2012, for their feedback on drafts of this article.

1. 132 S. Ct. 945 (2012).
2. *See infra* text accompanying notes 31–38.

made statements that call into question the Court's "third party doctrine," the controversial notion that government officials need no justification under the Constitution to view or access *any* activities or information that can be viewed or accessed by third parties outside the home.[3]

The decision in *Jones* is long overdue. Federal, state, and local governments are rapidly taking advantage of advances in technology to keep tabs on their citizenry, in increasingly intrusive ways. Millions of times each year, the police track individuals using technology attached to cars, as in *Jones*, or signals from either phones or factory-installed transponders.[4] Thousands of cameras, many with zoom, tracking, and facial recognition capacity, continuously scan hundreds of urban and suburban areas.[5] Equipped with powerful magnification devices, hundreds of drones will soon be flying over a number of jurisdictions.[6] The capacity of computers to access, store, and analyze data has made mountains of personal information—ranging from phone and e-mail logs to credit card and bank transactions—available to government officials at virtually the touch of a button.[7] Before *Jones*, the third party doctrine ensured that none of this activity was regulated by the Fourth Amendment.[8]

---

3. *Id.* For one of the more recent, among dozens of, criticisms of the third party doctrine, see generally Erin Murphy, *The Case Against the Third Party Doctrine: A Response to Epstein and Kerr*, 24 BERKELEY TECH. L.J. 1239 (2009).

4. *See, e.g.*, Justin Elliott, *Police Tapped Sprint Customer GPS Data 8 Million Times in a Year*, TPMMUCKRAKER (Dec. 4, 2009, 6:03 PM), http://tpmmuckraker.talkingpointsmemo.com/2009/12/ revelation_8_million_gps_searches_on_sprint_by_law.php.

5. *See, e.g.*, Mark Rockwell, *ACLU Calls for Ban on New Chicago Surveillance Cameras*, GOVERNMENT SECURITY NEWS (Feb. 8, 2011, 12:12 PM), http://www.gsnmagazine.com/node/22394 (reporting the presence of over 1,500 cameras in Chicago with zoom, tracking, and facial-recognition capacity); Allison Klein, *Police Go Live Monitoring D.C. Crime Cameras*, WASH. POST (Feb. 11, 2008), http://www.washingtonpost.com/wp-dyn/content/article/2008/02/10/AR2008021002726_pf.html (reporting seventy-three cameras in use, with fifty more planned, in Washington, D.C. and camera systems in Baltimore, Chicago, New York, and Philadelphia).

6. RICHARD M. THOMPSON II, CONGRESSIONAL RESEARCH SERVICE, DRONES IN DOMESTIC SURVEILLANCE OPERATIONS: FOURTH AMENDMENT IMPLICATIONS AND LEGISLATIVE RESPONSES 2–3 (2012), *available at* http://www.fas.org/sgp/crs/natsec/R42701.pdf (reporting that the FAA predicts that over 30,000 drones will be flying over domestic airspace within the next twenty years, equippable with "high-powered cameras, thermal imaging devices, license-plate readers, and laser radar (LADAR)" (footnotes omitted)).

7. *See* Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317, 318–21 (2008) (describing the expansion of federal, state, and private data mining initiatives despite the end of the Terrorism Information Awareness program in 2003).

8. For a description of some of the cases adopting the third party doctrine, see *infra* text accompanying notes 27–30.

Strictly speaking, even after *Jones* most of these investigative techniques remain unregulated as a constitutional matter. The precise holding of *Jones*, per Justice Scalia, was that when police officers attach a tracking device to a car, they are engaging in a trespass on an "effect" that is protected by the Fourth Amendment's declaration that "people shall be secure in their houses, persons, papers and effects from unreasonable searches and seizures."[9] While the majority went on to conclude that subsequent use of that device to track movements of the car constitutes a Fourth Amendment search,[10] the key to the decision is the predicate trespass. None of the investigative actions described above, except for the type of tracking involved in *Jones* itself, involve a physical interference with property, which is the usual definition of trespass.[11]

The majority did clearly hold, however, that if a trespass occurs, the fact that third parties can observe the vehicle is irrelevant; a search has occurred.[12] Moreover, five Justices in *Jones*—Justice Sotomayor in a solo concurring opinion and Justice Alito, joined by three others—were willing to go further. Justice Sotomayor wrote that, although unnecessary to decide the precise question at issue in *Jones*, the Court would eventually need to recognize the ease with which technology enables the government to acquire personal information, chill expressive and associational freedoms, and abuse its power, and she strongly suggested that tracking even in the absence of trespass infringes reasonable expectations of privacy.[13] Justice Alito similarly opined that "society'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."[14] In short, both concurring opinions endorsed what the lower court in *Jones* called the "mosaic theory" of the Fourth Amendment—the idea that certain types of governmental investigation enable accumulation of so many individual bits about a person's life that the resulting

9. United States v. Jones, 132 S. Ct. 945, 949 (2012).
10. *Id.*
11. *See infra* note 62.
12. *Jones*, 132 S. Ct. at 949. The majority also made the intriguing statement that "no case" supports the proposition that a government action that would otherwise be a search is not a search if it "produces only public information." *Id.* at 952.
13. *Id.* at 956–57 (Sotomayor, J., concurring).
14. *Id.* at 964 (Alito, J., concurring).

personality picture is worthy of constitutional protection.[15]

The opinions in *Jones* thus open the door to a more expansive Fourth Amendment. But the Court still has much to work out. At present, the mosaic theory is little more than a name.[16]

Taking a different tack than the voluminous literature that has grappled with this issue both before and after *Jones*,[17] this article proffers a statute that attempts to operationalize mosaic theory, relying on two more basic concepts that I have explored in other work. The first concept is the proportionality principle, the idea that the justification for a search should be roughly proportional to the intrusiveness of the search. The second is John Hart Ely's political process theory.[18] As applied to searches, this theory counsels that courts should generally defer to legislation authorizing searches of groups when the affected groups have meaningful access to the legislative process and the search is implemented in an even-handed fashion.[19]

Of course, numerous other theories of the Fourth Amendment exist and might apply in this context. Some of them are described and compared in the following discussion. In part, this article is an effort to persuade that these other theories do not work as well.

The primary goal of this article, however, is to provide a springboard for a much-needed codification of search-related doctrine. Among Western countries, the United States stands out in its failure to provide clear statutory statements of the law governing

---

15. United States v. Maynard, 615 F.3d 544, 562 (2010) ("As with the 'mosaic theory' often invoked by the Government in cases involving national security information, 'What may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene.'" (quoting CIA v. Sims, 471 U.S. 159, 178 (1985))), *aff'd sub nom.* United States v. Jones, 132 S. Ct. 945 (2012).

16. *See generally* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 110 MICH. L. REV. (forthcoming 2012), *available at* http://ssrn.com/abstract=2032821 (criticizing "mosaic theory").

17. One of the earliest purveyors of mosaic theory (although without using the label) was Richard H. McAdams, *Tying Privacy in Knotts: Beeper Monitoring and Collective Fourth Amendment Rights*, 71 VA. L. REV. 297, 318 (1985) ("[W]hen courts consider . . . [F]ourth [A]mendment rights, they should focus on both the aggregate of individual police encounters and the synergistic effects of pervasive police practice on society as a whole."). One of the latest analyses of the theory is found in Kerr, *supra* note 16 (manuscript at 1–3) (arguing that mosaic theory cannot be coherently implemented).

18. *See generally* JOHN HART ELY, DEMOCRACY AND DISTRUST: A THEORY OF JUDICIAL REVIEW (1980) (exploring political process theory).

19. *See infra* text accompanying notes 79–85.

police investigation.[20] Codification might be particularly useful in the surveillance setting. In his concurring opinion, Justice Alito stated, "[i]n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative."[21] He continued, "[a] legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way."[22] The statute proposed in this article provides an example of the kinds of nuances that must be resolved in order to work through the Fourth Amendment's application to governmental surveillance. At the same time, in many respects the statute goes beyond anything the Fourth Amendment requires, in either scope or detail. As such, it is truly legislative in import, not simply a summary of possible judicially created minimum requirements under the Fourth Amendment.

After describing more fully the questions left open by *Jones* and how that case intersects with various Fourth Amendment theories, this article sets out the proposed statute. The statute begins with definitions of terms like "search," "probable cause," and "exigent circumstances" and then proceeds to substantive regulation of "targeted" searches, relying on proportionality theory, and of "general" searches, relying on political process theory. Each provision is followed by a brief commentary. A number of other issues—most importantly regarding the use of information gathered through surveillance and sanctions for violations of the rules—are not addressed in the statute, but a few comments about these topics appear at the end of the article. Only by making explicit in this way the consequences of theory can theory be adequately evaluated.

II. QUESTIONS AFTER *JONES*

The story of the Supreme Court's conservative take on the definition of the word "search" in the Fourth Amendment is well-known. After years of defining this threshold question in property terms,[23] the Court reoriented search analysis toward a test focusing on

20. *Cf.* Craig M. Bradley, *Overview*, *in* CRIMINAL PROCEDURE: A WORLDWIDE STUDY xv, xix (Craig M. Bradley ed., 1999) ("[W]ith the exception of the United States, all of the countries presented in the book, and most other countries, have a nationally applicable code of criminal procedure rather than relying on judicial precedents as the means of governing the criminal process.").

21. United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring).

22. *Id.*

23. *See, e.g.*, Silverman v. United States, 365 U.S. 505, 511 (1961) (holding that use of a

reasonable expectations of privacy.[24] On its face, that test appears to be broader than a property-based approach, as evidenced by the decision in the seminal case of *Katz v. United States*,[25] which established privacy protection as the focus of Fourth Amendment protection. In that case, the Court held that electronic interception of a phone conversation taking place in a phone booth was a search despite the uncontroverted facts that the defendant did not own the booth, the bugging device would not have physically trespassed on it even if he had owned it, and the conversation intercepted was not an "effect."[26]

In the hands of the post-Warren Court, however, *Katz* has pretty much been limited to its facts in situations not involving a physical intrusion into a house, person, paper, or effect. The Fourth Amendment remains tied to property concepts, largely because the post-Warren Court has subscribed to the notion that, when a trespass is not involved, the police are entitled to view or access anything a third party can view or access. Thus, *Katz* did not prevent the Court from holding that no search occurs when police observe, from navigable airspace, the fenced-in curtilage of the home;[27] after all, the Court reasoned, members of the public in a plane or on a double-decker bus could have seen the same thing the police did.[28] Similar reasoning led the Court to decide that people assume the risk that when information is handed over to third parties—including institutional third parties such as banks and phone companies—they cannot reasonably expect the information to remain private.[29] In

---

"spike mike" that intruded into a wall was a trespass and therefore a search); Goldman v. United States, 316 U.S. 129, 134–35 (1942) (holding that use of a detectaphone that touched the outer wall of suspect's office was not a trespass and therefore not a search); Olmstead v. United States, 277 U.S. 438, 457, 464 (1928) (holding that tapping of telephone wires outside suspects' premises was not a trespass and therefore not a search).

24. *See* CHARLES H. WHITEBREAD & CHRISTOPHER SLOBOGIN, CRIMINAL PROCEDURE: AN ANALYSIS OF CASES AND CONCEPTS 120–21 (5th ed. 2008) (describing post-*Katz* developments).

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

26. *See id.* at 353 ("We conclude that . . . the 'trespass' doctrine . . . can no longer be regarded as controlling. . . . The fact that the electronic device employed to achieve that end did not happen to penetrate the wall of the booth can have no constitutional significance.").

27. California v. Ciraolo, 476 U.S. 207, 214 (1986).

28. *See id.* at 211 ("[A] 10-foot fence might not shield these plants from the eyes of a citizen or a policeman perched on the top of a truck or a two-level bus.").

29. Smith v. Maryland, 442 U.S. 735, 744 (1979) (holding that a person who "voluntarily convey[s] numerical information to the telephone company . . . assume[s] the risk that the company would reveal to police the numbers he dialed"); Miller v. United States, 425 U.S. 435, 443 (1976) (holding that government access to bank records is not a search because an

short, the third party doctrine has pervaded analysis of the search issue.[30]

The *Jones* majority departed from this line of cases, but only minimally so. The month-long tracking that occurred in *Jones* involved observation of public activity that could have been viewed by anyone and thus, under the third party doctrine, should have been exempted from Fourth Amendment restrictions. The Court held to the contrary, but only because the observation was facilitated by a physical trespass.[31] That reasoning comports with the property orientation of previous cases. In fact, Justice Scalia's opinion avoided the reasonable-expectation-of-privacy test entirely. While he did not repudiate that test,[32] he reasoned that, given the Fourth Amendment's reference to persons, houses, papers, and effects, the Amendment also explicitly protects property interests.[33] Thus, on the facts of *Jones*, the reasonable-expectation-of-privacy test was not needed to resolve the case.

In contrast, the five concurring Justices signaled a readiness to abandon the link between physical intrusion and the Fourth Amendment and hold that, even when a trespass is not involved, public surveillance using technology can be a search, at least when it is prolonged. Justice Alito, joined by Justices Ginsburg, Breyer, and Kagan, contended that the majority's approach was too beholden to outmoded property concepts and insisted that the only question that

---

individual "takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government," even where the information is "revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed").

30. The Court has actually developed three doctrines that implement the third party idea. The *knowing exposure* doctrine asks whether the activity observed by police was knowingly exposed to the public, and has bolstered decisions allowing tracking of cars and flyovers of open fields and curtilage. The *general public use* doctrine determines whether police, standing on a lawful vantage point, rely on technology that is generally available to the public; this doctrine might leave unregulated the use of binoculars to look inside a house. The *assumption of risk* doctrine posits that no search occurs when the government obtains information about a target from a third party that the target knows or should know has the information. *See* Christopher Slobogin, *Is the Fourth Amendment Relevant in a Technological Age? in* CONSTITUTION 3.0: FREEDOM AND TECHNOLOGICAL CHANGE 11, 14–19 (Jeffrey Rosen & Benjamin Wittes, eds., 2011).

31. *See* United States v. Jones, 132 S. Ct. 945, 949 (2012) ("We hold that the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search.'").

32. *See id.* at 952 ("The *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test." (emphasis added)).

33. *Id.*

should be asked is "whether the use of GPS tracking in a particular case involved a degree of intrusion that a reasonable person would not have anticipated."[34] Under this approach, Justice Alito continued, "relatively short-term monitoring of a person's movements on public streets" is not a search, but "the use of longer term GPS monitoring in investigations of most offenses" could be.[35] This language echoed that used by the lower court, which had held for Jones on the ground that "[w]hen it comes to privacy . . . the whole may be more revealing than the parts."[36]

Justice Sotomayor's position was, on the surface, similar to Justice Alito's and the lower court's. She thought the question should be "whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."[37] Going well beyond Justice Alito's concerns, however, she also stated that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties," an approach she considered "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[38]

Thus, after *Jones* five Justices are positioned to declare that long-term tracking is a search in the absence of a trespass, and the other four Justices have not definitively rejected that idea. However, several other questions remain open:

1. Will Justice Alito's distinction between long-term and short-term surveillance end up defining when a search occurs in public spaces, and if so, what is the difference between the two? In other words, how should mosaic theory play out? Justice Alito was unwilling to draw any robust conclusions on this score, other than to say that the four weeks involved in *Jones* "surely crossed" the line.[39]

34. *Id.* at 964 (Alito, J., concurring).
35. *Id.*
36. United States v. Maynard, 615 F.3d 544, 561 (D.C. Cir. 2010), *aff'd sub nom.* United States v. Jones, 132 S. Ct. 945 (2012).
37. *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring).
38. *Id.* at 957.
39. *Id.* at 964 (Alito, J., concurring).

2. If tracking is a search, does it always require probable cause? Although probable cause is usually required for a Fourth Amendment search,[40] neither the majority nor the concurring Justices in *Jones* flatly stated that the traditional rule applies to tracking.[41]
3. Assuming that probable cause or some other justification is usually required for technological tracking, at least if it is long-term, is that requirement relaxed or inapplicable in connection with investigation of "some offenses" (or "extraordinary offenses," the term Justice Alito used later in his opinion)?[42] If so, what offenses?
4. Reaching more broadly, does *Jones*'s treatment of tracking cases have implications for other situations that are encompassed by the third party doctrine, as Justice Sotomayor suggested? For instance, what if long-term tracking does not use technology? What if the government decides to access recorded data about a person that is possessed by a third party?

The statute proposed in this article will suggest answers to these questions. Before engaging in that relatively precise endeavor, however, it is necessary to flesh out some theoretical possibilities.

III. FOURTH AMENDMENT THEORY

Since *Katz*, the Supreme Court's focal point in determining whether a police action is a Fourth Amendment search has been privacy. Yet from its inception the reasonable-expectation-of-privacy test has been attacked as unduly manipulable. In his dissent in *Katz*, Justice Black complained that "by arbitrarily substituting the Court's language, designed to protect privacy, for the Constitution's language, designed to protect against unreasonable searches and seizures, the Court has made the Fourth Amendment its vehicle for holding all laws violative of the Constitution which offend the Court's broadest

40. *See* New Jersey v. T.L.O., 469 U.S. 325, 340 (1985) ("Ordinarily, a search—even one that may permissibly be carried out without a warrant—must be based upon 'probable cause' to believe that a violation has occurred.").

41. 132 S. Ct. at 954 (explaining that the Court had "no occasion to consider" the government's argument that something less than a warrant based on probable cause would have justified the search in *Jones*); *id*. at 964 n.11 (Alito, J., concurring) (stating that the question of what restrictions the Fourth Amendment imposes on tracking "is not before us").

42. *Id.* at 964.

concept of privacy."[43] While Justice Black did not agree with the defendant-oriented holding in *Katz*, he also presciently noted that the privacy concept could be abused in the government's favor as well.[44] Partly because they believe that the latter prediction has come to pass, many academic commentators have taken potshots at the reasonable-expectation-of-privacy test and proposed substitutes, including formulations focused on property,[45] coercion,[46] mutual trust,[47] liberty,[48] dignity,[49] security,[50] and power.[51]

There is no doubt that privacy is protean, given the whimsicality of public attitudes about disclosing personal facts and the increasing role technology plays in facilitating that disclosure.[52] Furthermore, as Justice Scalia has noted, the reasonable-expectation-of-privacy test is "circular," in the sense that expectations of privacy are reasonable only when the Court says they are.[53] I have argued that these

---

43. Katz v. United States, 389 U.S. 347, 373 (1967) (Black, J., dissenting).

44. *Id.* at 374 ("The history of governments proves that it is dangerous to freedom to repose such powers [provided by linking the Fourth Amendment to the "privacy" concept] in courts.").

45. *See* Morgan Cloud, *A Liberal House Divided: How the Warren Court Dismantled the Fourth Amendment*, 3 OHIO ST. J. CRIM. L. 33, 72 (2005) (arguing for a Fourth Amendment "rooted in property theories").

46. *See* William J. Stuntz, *Privacy's Problem and the Law of Criminal Procedure*, 93 MICH. L. REV. 1016, 1020 (1995) ("Were the law of criminal procedure to focus more on force and coercion and less on information gathering . . . it would square better with other constitutional law and better protect the interests most people value most highly.").

47. *See* Scott E. Sundby, *"Everyman"'s Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?*, 94 COLUM. L. REV. 1751, 1758–63 (1994) ("[T]he animating principle which has been ignored in the current Fourth Amendment debate is the idea of reciprocal government-citizen trust.").

48. Thomas P. Crocker, *From Privacy to Liberty: The Fourth Amendment after* Lawrence, 57 UCLA L. REV. 1, 4 (2009) ("*Lawrence*'s emphasis on liberty provides a fruitful way of reorienting Fourth Amendment protections when considering particular kinds of interpersonal relationships." (referencing Lawrence v. Texas, 539 U.S. 558 (2003))).

49. *See* John D. Castiglione, *Human Dignity Under the Fourth Amendment*, 2008 WIS. L. REV. 655, 661 ("[T]he concept of dignity captures a core Fourth Amendment value that privacy does not, and therefore must be explicitly incorporated into reasonableness analysis.").

50. Thomas K. Clancy, *What Does the Fourth Amendment Protect: Property, Privacy or Security?* 33 WAKE FOREST L. REV. 307, 307–08 (1998) ("Only by understanding the meaning of the term 'secure' is it possible to determine the scope of the Fourth Amendment's protections for individuals and, correlatively, the amount of unregulated governmental power the amendment allows.").

51. *See* Raymond Shih Ray Ku, *The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance*, 86 MINN. L. REV. 1325, 1326 (2002) ("The Fourth Amendment protects power not privacy.").

52. *See, e.g.*, Sundby, *supra* note 47, at 1758–63 ("The very notion of a right to be left alone seems a bit tattered once placed in the context of contemporary life.").

53. *See* Kyllo v. United States, 533 U.S. 27, 34 (2001) (observing that the reasonable-expectation-of-privacy test "has often been criticized as circular, and hence subjective and

objections can be partially overcome by tying privacy to positive law (including the law of property) and to empirical work on society's views.[54] But it must be admitted that privacy is a very elastic concept.

Most of the other tests fare no better, however. Terms like "liberty," "dignity," "power," "coercion," "trust," and "security" are hardly self-defining. And most of them do not help advance the ball. The entire Bill of Rights, from the First Amendment's guarantees of speech and association through the Eighth Amendment's prohibition on cruel and unusual punishment, is meant to protect liberty and dignity against governmental abuse of power. The issue in Fourth Amendment cases is the precise aspects of dignity, liberty, and power that are implicated by *searches and seizures*.[55] Protection against physical coercion cannot be the answer if we want covert surveillance to be regulated.[56] And maximizing citizen trust of government or the security of citizens from its officials, while certainly reasons to require justification for searches, does not tell us when something is a search or what justification is required if it is a search.[57]

That leaves property as a possible alternative touchstone for the Fourth Amendment, a notion that has taken on new life since Justice Scalia explicitly rejuvenated it in *Jones*. Several commentators have argued that property law provides a more concrete reference point for Fourth Amendment analysis than privacy does.[58] But property

---

unpredictable").

54. CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 32–35 (2007).

55. Thus Professor Ku, who argues that power is the linchpin of Fourth Amendment analysis, nonetheless circles back to privacy in defining why power is relevant. *See* Ku, *supra* note 51, at 1326 ("[T]he amendment is best understood as a means of preserving the people's authority over government—the people's sovereign right to determine how and when government may intrude into the lives and influence the behavior of its citizens."). Most critics of *Katz* seem more bothered by the way the Court defines privacy than by privacy's mismatch with the Fourth Amendment. *See, e.g.*, Castiglione, *supra* note 49, at 660 ("As courts' decisions have moved towards an almost exclusive focus on privacy as the counterbalance to the government's law-enforcement interest, the government's interests have increasingly prevailed and the sphere of protection afforded to the individual has shrunk." (footnote omitted)).

56. *See* SLOBOGIN, *supra* note 54, at 26 (noting that covert surveillance does not involve coercion).

57. *Id.* at 25 (discussing why the trust model, and by implication models focused solely on security, do not provide help in figuring out the justification required by the Fourth Amendment in particular situations).

58. For a post-*Jones* example of this stance, see Erica Goldberg, Commentary, *How* United States v. Jones *Can Restore Our Faith in the Fourth Amendment*, 110 MICH. L. REV. FIRST IMPRESSIONS 62, 68 (2012) (concluding that *Jones*'s "resurrection of the link between searches and property . . . is a substantial step toward" making the Fourth Amendment "more concrete").

notions are also manipulable and changeable, and thus their content for Fourth Amendment purposes will, as with expectations of privacy, be entirely dependent on what the Court says. For instance, the Court has held that private property in the "open fields" is not part of the house protected by the Fourth Amendment,[59] that garbage left at curbside is abandoned,[60] and, prior to *Katz*, that bugging a phone line outside of a house is not a trespass.[61]

For those who want to expand the scope of the Fourth Amendment to cover technological surveillance, property is a particularly shaky basis for reform. Justice Scalia's statement in *Jones* that planting a GPS device on a car is a trespass has been castigated as inconsistent with both the historical and the modern understanding of trespasses on chattel, which usually requires significant physical interference with property.[62] Scholars attempting to bring other types of surveillance under the property rubric have had to resort to even more exotic arguments. Interception of phone or computer communications, and tracking using the signals from cell phones, are said to be "trespasses" on the electronic particles sent by these devices.[63] Aerial surveillance purportedly violates the common law doctrine of *ad coelum*, which grants property rights directly above one's home (but, unfortunately for those who would like to regulate satellite and drone surveillance, nowhere else).[64] And perhaps most

---

59. *See, e.g.*, Oliver v. United States, 466 U.S. 170, 177 (1984) ("[O]nly the curtilage, not the neighboring open fields, warrants the Fourth Amendment protections that attach to the home.").

60. *See, e.g.*, California v. Greenwood, 486 U.S. 35, 40–41 (1988) ("[H]aving deposited their garbage 'in an area particularly suited for public inspection and, in a manner of speaking, public consumption, for the express purpose of having strangers take it,' respondents could have had no reasonable expectation of privacy in the inculpatory items that they discarded." (quoting United States v. Reicherter , 647 F.2d 397, 399 (3d Cir. 1981))).

61. *See* Olmstead v. United States, 277 U.S. 438, 457, 464 (1928) ("The insertions were made without trespass upon any property of the defendants. . . . The evidence was secured by the use of the sense of hearing and that only.").

62. *See, e.g.*, Peter A. Winn, *Trespass and the Fourth Amendment: Some Reflections on* Jones, USVJONES.COM (June 4, 2012), http://usvjones.com/2012/06/04/trespass-and-the-fourth-amendment-some-reflections-on-jones/ (noting that, according to Blackstone, trespass to chattels required that the chattel "had been misappropriated or destroyed," which clearly did not occur in *Jones*, and noting further that Justice Alito misquoted the relevant eighteenth-century treatise, which is actually hostile to the notion of a cause of action arising from trespass to chattels).

63. *See* Goldberg, *supra* note 58, at 68 ("Even in the *Katz* electronic surveillance case, the Court could have retained the connection between property rights and privacy rights by holding that an electronic connection to an individual's property (or to the phone company's property) is a physical intrusion, albeit on a microscopic level.").

64. Lance Polivy, *Property Expanding Fourth Amendment Protections: The Common Law*

creative of all is the assertion that people have a property interest in records created and maintained by third parties.[65]

I am sympathetic with the outcomes of these arguments. But they have a legal fiction quality to them that is as tenuous as any argument based on privacy. Furthermore, any realistic property-based Fourth Amendment is likely to leave intact the most egregious aspect of the third party doctrine: its immunization of governmental acquisition of personal information held by third parties.[66] I have contended that, with all of its flaws, privacy—defined loosely as the ability to avoid intrusion into one's affairs—remains the best basis for analyzing Fourth Amendment issues.[67] On this assumption, I have taken the position that any government effort to observe or find out about a person's activities, transactions, or communications is a Fourth Amendment search.[68] While this position is admittedly a significant departure from the Court's approach, it conforms to the lay use of the word "search," which, as Justice Scalia noted in *Kyllo v. United States*,[69] means "[t]o look over or through for the purpose of finding something; to explore; to examine by inspection."[70]

As Justice Scalia goes on to suggest in his *Kyllo* majority opinion, the Court's unwillingness to define search according to its plain meaning may be the result of a desire "to preserve somewhat more intact our doctrine that warrantless searches are presumptively unconstitutional."[71] In other words, because Fourth Amendment jurisprudence usually requires a warrant based on probable cause for any action denominated a search, the Justices are loath to apply the search label to police actions—like looking into a house from the

---

Doctrine of Ad Coelum *and Drone Searches after* Jones, USVJONES.COM (June 3, 2012), http://usvjones.com/2012/06/03/property-expanding-fourth-amendment-protections-the-common-law-doctrine-of-ad-coelum-and-drone-searches-after-jones.

65. That is not to say an argument cannot be made in some contexts. *See, e.g.*, Jerry L. Mashaw, *"Rights" in the Federal Administrative State*, 92 YALE L.J. 1129, 1137 (1983) ("The Freedom of Information Act and the Privacy Act gave all citizens 'property rights' in the information held by government bureaus." (footnotes omitted)).

66. *See* Winn, *supra* note 62 ("[T]he law of trespass, if it requires anything, requires a possessory interest; and the powerful intuitions of invasion of privacy today are triggered by the massive amounts of detailed personal information residing in the servers of third parties.").

67. *See* SLOBOGIN, *supra* note 54, at 23–24 (explaining "why privacy is a core value protected by the Fourth Amendment").

68. *See id.* (arguing that the word "search" for Fourth Amendment purposes ought to be congruent with the lay definition of the term).

69. 533 U.S. 27 (2001).

70. *Id.* at 32 n.1.

71. *Id.* at 32.

public sidewalk—that are often reasonable attempts to *develop* probable cause. Even liberal Justices have had a hard time ignoring this reality.[72]

Another approach—again suggested by Justice Scalia in *Kyllo*—would be to adopt a broad definition of search, as described above, but to declare that certain searches are reasonable even when not based on probable cause.[73] For some time I have been advancing an analogous approach, which I have called the proportionality principle.[74] Simply put, the proportionality principle requires that the justification for a search be roughly proportional to its intrusiveness. The Court has always used this proportionality reasoning in dealing with seizures,[75] and on more than a few occasions the Court appears to have applied it to searches.[76] In *Jones* itself, Justice Alito's distinction between "prolonged" and short-term tracking could be seen as an application of the proportionality idea. The suggestion here is that this principle—although not necessarily the Court's application of it—should be adopted as the means of determining the "reasonableness" of *all* searches.

However, I have also suggested two exceptions to the proportionality principle. First, the justification normally required by that principle should be relaxed when the search is designed to deal with a significant, imminent, and specific threat.[77] The law, including

---

72. For instance, both Justice Brennan and Justice Marshall joined *United States v. Knotts*, holding that short-term tracking with a beeper is not a search, and only Justice Marshall was "adamant" about requiring a warrant in *Miller* and *Smith*, the bank record and phone record cases. SLOBOGIN, *supra* note 54, at 208.

73. *Kyllo*, 533 U.S. at 30–32.

74. The first article advocating this position was Christopher Slobogin, *The World Without a Fourth Amendment*, 39 UCLA L. REV. 1, 68–75 (1991).

75. *See, e.g.*, Michigan v. Summers, 452 U.S. 692, 697–98 (1981) (noting that in seizure cases that did not require probable cause, the Court has held that "the intrusion on the citizen's privacy 'was so much less severe' than that involved in a traditional arrest that 'the opposing interests in crime prevention and detection and in the police officer's safety' could support the seizure as reasonable" (quoting Dunaway v. New York, 442 U.S. 200, 209 (1979)).

76. *See, e.g.*, O'Connor v. Ortega, 480 U.S. 709, 725 (1987) (stating that reasonable suspicion is sufficient to justify search of an employee's desk in part because "the employer intrusions at issue here 'involve a relatively limited invasion' of employee privacy" (quoting Camara v. Mun. Court of San Francisco, 387 U.S. 523, 537 (1967)); *see also* Terry v. Ohio, 392 U.S. 1, 27 (1968) ("[T]here must be a narrowly drawn authority to permit a reasonable search for weapons for the protection of the police officer, . . . regardless of whether he has probable cause to arrest the individual for a crime.").

77. *See* SLOBOGIN, *supra* note 54, at 26–28 ("Prevention of imminent harm is clearly a legitimate government objective. In the post-9/11 era, the danger rationale for reducing the government's burden is particularly attractive.").

Fourth Amendment law, routinely relaxes restrictions on the government when its aim is to *prevent* serious harm.[78]

The second exception arises when the government wants to search large groups of predominately law-abiding people, as occurs in connection with drug testing programs, citywide camera systems, or a nationwide data-mining regime. Under today's jurisprudence, many of these programs (for instance, camera surveillance of public streets and mining information held by third parties) would not be considered searches at all.[79] When they are said to be searches (as with drug testing), the Supreme Court's approach has been to apply its "special needs" analysis, which has generally meant that so long as the government can demonstrate the group search meets a significant governmental need that is distinct from a general interest in crime control, it is permissible despite the lack of individualized suspicion.[80] Academics have generally disagreed with the Court's holdings but have usually resorted to similar analysis in such cases by requiring the government to show that the search program addresses a *particularly* significant regulatory problem in the *least intrusive* manner possible.[81]

I am not as confident that courts are equipped to measure the necessity for a group search or the usefulness and feasibility of its alternatives.[82] In any event, I have suggested that application of John Hart Ely's political process theory should be considered in this

78. *See, e.g.*, Addington v. Texas, 441 U.S. 418, 429 (1979) (permitting commitment on clear and convincing evidence rather than proof beyond a reasonable doubt partly because the state should not be saddled with a standard of proof that "may completely undercut" its preventive efforts); *see also Terry*, 392 U.S. at 27 (justifying frisks based on reasonable suspicion in part because of the need to protect the police).

79. *See supra* text accompanying notes 27–30.

80. *Compare* Bd. of Educ. v. Earls, 536 U.S. 822, 836 (2002) (holding that suspicionless drug testing of students in extracurricular activities was permissible "[g]iven the nationwide epidemic of drug use, and the evidence of increased drug use in Tecumseh schools"), *with* City of Indianapolis v. Edmond, 531 U.S. 32, 41–42 (2000) (holding that suspicionless stops at roadblocks set up to interdict drugs were unconstitutional because "the primary purpose of the . . . program is to uncover evidence of ordinary criminal wrongdoing").

81. *See, e.g.*, Thomas Clancy, *The Role of Individualized Suspicion in Assessing the Reasonableness of Searches and Seizures*, 25 MEMPHIS L. REV. 483, 618 (1995) (arguing that group searches ought to be analyzed by looking at "the absence of effective alternatives, the comparative productivity of operating without individualized suspicion, the need to achieve a high level of enforcement, and the inability to identify the source of the problem utilizing individualized suspicion"); *see also* Scott Sundby, *A Return to Fourth Amendment Basics: Undoing the Mischief of* Camara *and* Terry, 72 MINN. L. REV. 383, 430–36 (1988) (arguing for application of a "compelling government interest-least intrusive means test" for "initiatory searches" for which there is no pre-existing suspicion).

82. *See* Slobogin, *supra* note 30, at 28–29 (providing examples of why judicial analysis of the feasibility and efficacy of differing law enforcements will be very difficult).

context.[83] Ely argued that, when interpreting vague constitutional provisions such as the Due Process Clause, courts should grant deference to legislative pronouncements—in other words, engage only in rationality review—if the affected groups had meaningful access to the legislative process and the statute is framed and applied even-handedly.[84] Applying this analysis in the Fourth Amendment context, a statute authorizing a group search might be presumptively valid. However, a group search program initiated solely by the executive branch is not entitled to judicial deference. Furthermore, even when authorized by legislation, such programs are vulnerable under political process theory if the affected group lacked representation in the decision-making body. Although the latter inquiry can be complex,[85] in the search context it can be operationalized in part by assuring that members of the decision-making body are subject to the program.

This discussion of Fourth Amendment theory has been an extremely brief summary of longer treatments.[86] These more detailed works explain why the proportionality principle, the danger exception to that principle, and political process theory are consistent with the fundamental values underlying the Fourth Amendment and why the restrictions they impose on investigative techniques that the Court has seen fit to leave unregulated are important. Enough has been said here, however, to set up the next section of this article, which presents a statute designed to implement these three concepts.

IV. A PROPOSED STATUTE

The following statute is divided into two parts: a definition section and a section setting forth substantive rules governing the conduct of searches. To a large extent, it is meant to provide one possible implementation of the concurring opinions in *Jones*. It rejects the

83. Christopher Slobogin, *Government Dragnets*, 73 LAW & CONTEMP. PROBS. 107, 130–38 (2010).

84. ELY, *supra* note 18, at 102.

85. *See* Slobogin, *supra* note 83, at 132–36 (discussing public choice issues). It is also possible that a group search program permissible under political process theory could still be struck down on First Amendment grounds. *Cf.* Thomas P. Crocker, *The Political Fourth Amendment*, 88 WASH. U. L. REV. 303, 375 (2010) (suggesting that the Fourth Amendment, read through a First Amendment prism, might require nullification of laws that chill collective activity like association and speech, despite the third party doctrine).

86. A longer summary is found in Slobogin, *supra* note 30, at 23–31. For more on the proportionality principle, see SLOBOGIN, *supra* note 54, at 23–47. For more on the application of political process theory to the Fourth Amendment, see Slobogin, *supra* note 83, at 130–38.

Court's third party doctrine and accepts the "mosaic" notion that accumulation of publicly available information or information in the hands of third parties can be a search.

However, the statute also goes well beyond the innuendo in the concurring opinions in *Jones*. It regulates not only physical surveillance (for instance, tracking and camera surveillance) but also transaction surveillance (for instance, accessing digitized information). It also makes an important distinction between targeted searches and general searches, with the former regulated under proportionality theory and the latter regulated under political process theory. As a result, in some places (for instance, the definition of "search" or the regulation of non-technological searches) the statute provides more protection than even a broad interpretation of the *Jones* opinions would contemplate; in others (for instance, the regulation of general searches) it may provide more or less protection than the Fourth Amendment does, depending on the context and how the Court's precedents are interpreted. Each provision is followed by a short commentary explaining the black letter language and tying the provision to previous discussion.

REGULATION OF SURVEILLANCE TECHNIQUES

PART I: Definitions

(1) Search: An effort by government to find or discern evidence of unlawful conduct. A targeted search seeks to obtain information about a specific person or circumscribed place. A general search seeks to obtain information about people or places that are not targets at the time of the search.

Commentary: The definition in this provision is broader than the Supreme Court's definition of search for Fourth Amendment purposes. Rather than focusing on reasonable expectations of privacy and trespass, it straightforwardly defines search the way a layperson would and consistently with the plain meaning of the Fourth Amendment.[87] It rejects the implications of the third party doctrine.

87. As such, this definition is very similar to a suggestion made by Daniel Solove. *See* Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1514 (2010) ("[T]he Fourth Amendment should provide protection whenever a problem of reasonable significance

Crucial to note is that the definition does not differentiate between searches using technology and searches with the naked eye. The officer who watches an individual walking down the street to see what transpires is conducting a search under this definition whether she does so with her unaided vision, binoculars, closed-circuit television, or a drone. The officer who peruses records is engaged in a search whether he does so manually or with a computer. Thus, this provision avoids tying the definition of search to problematic assessments of the search method used—such as whether it is general public use, enhances the normal capacity of the police, or is unusually pervasive or disruptive—that have bedeviled the courts.[88] It also avoids tying the definition of search to whether and to what extent a physical intrusion is involved, whether the target has taken sufficient steps to enhance privacy, or whether the item or information sought is "intimate" as opposed to impersonal—all imponderable factors the courts have nonetheless felt compelled to consider under the Supreme Court's test.[89]

The subcategories of search defined in this provision are necessary for the purposes indicated in Part II, which treats targeted searches differently than general searches. Note that targets can be not only people but places. While targeted searches will usually be directed at a suspect, in some cases the target may be a place associated with criminal activity rather than a person; if so, however, this definition requires that the place be "circumscribed" (small and limited) to distinguish it from a general search. Note further that if information is sought from third parties about a specific person or place, it is a targeted search. If, on the other hand, the government is trying to solve, prevent, or deter as-yet undetected or perpetrated crime through surveillance of the general population or a subset of it, it is carrying out a general search.

(2) <u>Data Search</u>: A search, in the absence of explicit consent, of digital, paper, audio, or other information sources and records that is not governed by 18 U.S.C. § 2510 (Title III).

---

can be identified with a particular form of government information gathering.").

88. *See* Christopher Slobogin, *Technologically-Assisted Physical Surveillance: The American Bar Association's Tentative Draft Standards*, 10 HARV. J.L. & TECH. 383, 394–98 (1997) (discussing factors courts consider in determining whether a particular type of surveillance constitutes a search).

89. *Id.* at 392–94.

Commentary: This definition encompasses accessing—through technological or non-technological means—phone and e-mail logs, bank records, credit card records, and any other records, but not interception of the content of phone or computer communications. The latter type of search generally requires a special warrant and is governed by Title III.

(3) Public search: A search of a place, in the absence of explicit consent, focused on activities or persons, limited to what the natural senses of a person on a lawful public vantage point could discern at the time of the search.

Commentary: This definition encompasses surveillance—whether unaided or relying on technology such as closed-circuit television, drones, and tracking and magnification devices—of curtilage and home interiors as well as of public places, provided that the surveillance discerns only what the natural senses could have discerned from a lawful vantage point. Thus, a naked-eye or technologically-enhanced search of a home interior by an officer standing on the curtilage would not be a *public* search. Nor would a technologically-enhanced search of a home interior, curtilage, or a public place be a public search—even if it took place from a lawful vantage point—if it observed activity that could not have been seen by the naked eye from a legitimate position at the time of the search.[90] Most obviously, a search would not be public if it involves using technology that can detect items underneath clothing or through opaque surfaces of cars and buildings.[91]

In all of these situations, the provisions on public searches detailed in Part II do not apply. Generally, a warrant based on probable cause would be required, although there may be exceptions. In *United States v. Place*,[92] the Court held that a dog-alert to the presence of contraband is not a search because it is "much less intrusive" than a

90. This notion could raise some difficult issues. *Cf.* SLOBOGIN, *supra* note 54, at 64 (stating that if the police did not resort to naked-eye viewing because they feared discovery, thus leading the targets to stop what they were doing or to hide it better, "the interior details arguably could *not* have been seen with the naked eye").

91. *See* Richard S. Julie, *High-Tech Surveillance Tools and the Fourth Amendment: Reasonable Expectations of Privacy in the Technological Age*, 37 AM. CRIM. L. REV. 127, 139–40 (2000) (describing concealed weapon detectors' capability generally and, more specifically, a device from Millivision that detects silhouettes against radiation waves emitted by the body to detect items underneath clothing).

92. 462 U.S. 696 (1983).

typical search,[93] and involves only the disclosure of an item in which, a later case explained, there is "no legitimate privacy interest."[94] Under the definition of "search" in these provisions, the dog sniff in *Place* would be a search, but might be considered reasonable given the lesser infringement on privacy.[95]

(4) Probable cause: An articulable belief that a search will more likely than not produce contraband, fruit of crime, or other significant evidence of wrongdoing. The belief may be based on statistical analysis. Judicial authorization for a search based on probable cause is called a warrant and must describe with particularity the person or place targeted, the evidence sought, and, if applicable, the duration of the search. A warrant is valid for 30 days, at which point a new showing of probable cause must be made.

Commentary: The Supreme Court's definition of probable cause is extremely vague. An oft-quoted passage from the Court states that probable cause exists where "the facts and circumstances within [the officers'] knowledge and of which they had reasonably trustworthy information [are] sufficient in themselves to warrant a man of reasonable caution in the belief" that evidence of crime will be found.[96] In the case in which this language appeared, the evidence was contraband.[97] In dictum in another case, the Court stated that probable cause would exist even if the items sought are simply "useful as evidence of a crime."[98]

The definition in this provision is more precise, and perhaps more demanding, in two ways. First, it adopts the preponderance standard, which is likely the way most judges think about probable cause.[99]

93. *Id.* at 707 (concluding, in dictum, that a dog sniff of luggage is not a search).

94. United States v. Jacobsen, 466 U.S. 109, 123 (1984).

95. The Court will be addressing this issue in more detail in Florida v. Jardines, No. 11-564 (U.S. argued Oct. 31, 2012), to be decided in the 2012–13 Term. The Florida Supreme Court in *Jardines* held that a dog sniff of a home conducted from the front door of the residence is a Fourth Amendment search requiring probable cause. Jardines v. State, 73 So. 3d 34, 37 (Fla. 2011). *Jones* suggests that a key inquiry will be whether the presence of the dog is a trespass on curtilage or instead can be viewed as justified through "consent" implied by the presence of a sidewalk to the front door and other indicia of welcome.

96. Carroll v. United States, 267 U.S. 132, 162 (1925).

97. Specifically, the item seized was "intoxicating liquor" being transported during the Prohibition era. *Id.*

98. Texas v. Brown, 460 U.S. 730, 742 (1983).

99. *See* Max Minzer, *Putting Probability Back into Probable Cause*, 87 TEX. L. REV. 913,

Second, the definition also requires that the search seek significant evidence of wrongdoing, such as contraband, stolen property, or direct visual or written proof of crime, rather than mere circumstantial proof of a prohibited harm. Thus, under this definition, even a demonstration by a preponderance of the evidence that a search will prove gang membership would not constitute probable cause,[100] nor would a more-likely-than-not showing that a search will reveal that the target frequents a particular place or knows certain people. Conversely, a demonstration by a preponderance that a search will allow observation of criminal conduct or produce illegal drugs or a murder weapon would constitute probable cause under this definition.

This provision and the next provision also recognize that suspicion may be based on an algorithm or profile that produces a fifty percent hit rate (a quantification of the preponderance standard).[101] This situation could arise, for instance, if the government can demonstrate, using crime-mapping data, a more-likely-than-not probability that a crime will occur in a particular, well-circumscribed area during the period of the authorization.[102]

The definition of "warrant" tracks the Fourth Amendment's language, adjusted for the surveillance context. The thirty-day limitation is analogous to the durational limitation imposed on electronic surveillance warrants.[103] It ensures that prolonged surveillance will be supported by periodically renewed individualized or statistical justification.

---

927 n.62 (2009) ("A 1982 survey of 166 federal judges asked their view of the numeric equivalent of probable cause and found a mean level of 45.8% and a median of 50%.").

100. *Cf.* Messerschmidt v. Millender, 132 S. Ct. 1235, 1251 (2012) (Kagan, J., concurring in part and dissenting in part) (arguing, in a case where the majority held that a reasonable officer could have believed there was probable cause to seize evidence of gang membership from the Millenders' home, that "[m]embership in even the worst gang does not violate California law").

101. *See, e.g.*, Brown v. Bowen, 847 F.2d 342, 345 (7th Cir. 1988) (stating that, under the preponderance standard, "the trier of fact rules for the plaintiff if it thinks the chance greater than 0.5 that the plaintiff is in the right").

102. *Cf.* Andrew Guthrie Ferguson & Damien Bemache, *The "High-Crime Area" Question: Requiring Verifiable and Quantifiable Evidence for Fourth Amendment Reasonable Suspicion Analysis*, 57 AM. U. L. REV. 1587, 1631–35 (2008) (discussing methods of defining a "high-crime area" using data).

103. *See* Electronic Communication Privacy Act, 18 U.S.C.A. § 2518(5) (West 2012).

(5) Reasonable suspicion: An articulable belief that a search will more likely than not lead to evidence of wrongdoing. The belief may be based on statistical analysis. Judicial authorization for a search based on reasonable suspicion is called a court order and must describe with particularity the person or place targeted, the evidence sought, and, if applicable, the duration of the search. A court order is valid for 48 hours, at which point a new showing of reasonable suspicion must be made.

Commentary: The Court has indicated that the reasonable suspicion standard is more easily met than the probable cause standard, but otherwise has provided little guidance beyond insisting that the police have more than an "inchoate or unparticularized suspicion or 'hunch.'"[104] The present definition more precisely communicates that reasonable suspicion is a lower standard than probable cause by referring to an action's capacity to "lead" to evidence (rather than produce "significant" evidence), which is often the goal of surveillance. For instance, in *In re Application of the United States*,[105] the court held that a warrant could not issue merely to obtain location data about an individual suspected of crime, because location is not "evidence of a crime."[106] However, under the standard in this provision, if the government can show that it has probable cause to arrest the individual, discovery of his location would more likely than not lead to evidence that will help prove wrongdoing, i.e., it will lead to discovery of the suspect, and thus reasonable suspicion would exist.

Given the language of the Fourth Amendment, a warrant must be based on probable cause. However, the Supreme Court has suggested that courts are able to issue orders authorizing searches or seizures on less than probable cause.[107] Current statutes, such as the Electronic Communication Privacy Act, also authorize court orders based on varying levels of justification.[108] This provision similarly authorizes

104. Terry v. Ohio, 392 U.S. 1, 27 (1968).

105. No. 10-2188-SKG, 2011 WL 3423370 (D. Md. Aug. 3, 2011).

106. *Id.* at *7 ("Fourth Amendment jurisprudence [does not] sanction[] access to location data on the basis of an arrest warrant alone . . . where there is no evidence of flight to avoid prosecution and the requested information does not otherwise constitute evidence of crime.").

107. *Cf.* Hayes v. Florida, 470 U.S. 811, 817 (1985) ("[T]he Fourth Amendment might permit the judiciary to authorize the seizure of a person on less than probable cause . . . ."); United States v. Karo, 468 U.S. 705, 718 n.5 (1984) (referencing this possibility with respect to tracking inside a home).

108. *See* 18 U.S.C.A. § 2703(d) (West 2012) (authorizing access to account logs and e-mail addresses, etc. if a court finds "specific and articulable facts showing that there are reasonable

court orders based on reasonable suspicion. The forty-eight-hour limitation on the validity of a court order is necessary given the provisions on targeted searches in Part II.

(6) Exigent circumstances: (a) Circumstances that augur a serious and specific danger, in which case a search is permitted if a reasonable law enforcement officer would believe it is necessary to help avert the perceived danger; or (b) circumstances involving imminent danger or disappearance of evidence that make obtaining a warrant or court order in a timely manner difficult, in which case only probable cause or reasonable suspicion, as the case may be, is required prior to the search.

Commentary: Subsection (a) implements the danger exception discussed earlier.[109] It is meant to encompass national security crises and other significant emergencies, imminent or not. Subsection (b) is a standard definition of exigency focused on whether there is time to get an order.[110] Subsection (a) is the only bow to Justice Alito's suggestion in *Jones* that investigative techniques normally governed by the Fourth Amendment should not be subject to constitutional regulation when used to investigate "extraordinary offenses."[111] Otherwise, this definition of exigent circumstances does not relax restrictions on searches based on the nature of the offense. This stance is based on the assumption that a search for evidence of an already-committed crime does not merit less regulation simply because the crime is a serious one.[112]

---

grounds to believe that . . . the records or other information sought are relevant and material to an ongoing criminal investigation").

109. *See supra* text accompanying notes 77–78.

110. *See* Minnesota v. Olson, 495 U.S. 91, 100 (1990) (indicating that the "correct standard" for gauging exigency justifying a warrantless intrusion is whether there is "hot pursuit of a fleeing felon, or imminent destruction of evidence, or the need to prevent a suspect's escape, or the risk of danger to the police or to other persons inside or outside the dwelling" (citation omitted) (quoting State v. Olson, 436 N.W.2d 92, 97 (Minn. 1989))).

111. United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring).

112. For a lengthier argument, see generally Christopher Slobogin, *Why Crime Severity Analysis is Not Reasonable*, 97 IOWA L. REV. BULL. 1 (2012).

PART II: Regulation

(1) Targeted Public Searches

(a) A targeted public search that lasts longer than 48 hours in aggregate requires probable cause, and a warrant unless exigent circumstances exist.

(b) A targeted public search that lasts longer than 20 minutes in aggregate but no longer than 48 hours in aggregate requires reasonable suspicion, and a court order unless exigent circumstances exist.

(c) A targeted public search that does not last longer than 20 minutes in aggregate may occur at a law enforcement officer's discretion whenever the officer believes in good faith that the search can accomplish a legitimate law enforcement objective.

Commentary: The concurring opinions in *Jones* suggest that mosaic theory is in play when the government targets an individual. If so, some method of measuring the intrusiveness of aggregated information is necessary. But neither Justice Sotomayor nor Justice Alito attempt to explain how that theory might be implemented. Doing so requires addressing a number of complicated issues. Professor Orin Kerr, who is not a fan of mosaic theory, has compiled a list of these issues, which includes: (1) What test determines when a mosaic has been created? (2) How should non-continuous surveillance be analyzed? (3) What surveillance techniques are governed by mosaic theory? (4) What level of justification is required to carry out a mosaic search?[113] Professor Kerr believes that these questions are "difficult and novel" and counsel against adopting mosaic theory.[114]

These questions *are* difficult and novel. But this provision, in combination with the definitions already provided, does a passable job of answering them. Its implementation of mosaic theory is based on application of the proportionality principle's stipulation that the justification for a search be roughly proportional to its intrusiveness. Taking a cue from Justice Alito's use of the word "prolonged" to

113. *See* Kerr, *supra* note 16 (manuscript at 19–20).
114. *Id.* (manuscript at 3).

describe the types of tracking he might consider a search,[115] the provision's restrictions do not depend on the type of technique at issue but rather rely on time as the relevant metric for determining intrusiveness. The provision draws the probable cause line at forty-eight hours, the length of time the government may hold an arrestee before a judge must be consulted.[116] It draws the reasonable suspicion line at twenty minutes, the outer limits of a permissible length of a street stop.[117] Targeted public searches that last less than twenty minutes must still be justified, but need only be in pursuit of any "legitimate law enforcement objective."[118] Breaks in surveillance do not "restart the mosaic clock,"[119] but are aggregated to determine whether the twenty-minute or forty-eight-hour threshold is met.

Note that this provision does not require as much justification as would be required for physical seizures of equivalent duration. A seizure that goes beyond twenty minutes usually becomes the functional equivalent of an arrest and thus requires probable cause, and a confrontation of less than twenty minutes that is nonetheless considered a seizure requires reasonable suspicion.[120] The assumption here, however, is that physical detentions are more intrusive than "virtual searches" of the type addressed in this provision.[121] Thus, under proportionality reasoning, the justification required is ratcheted downward.

---

115. *See Jones*, 132 S. Ct. at 964 (Alito, J., concurring).

116. *See* County of Riverside v. McLaughlin, 500 U.S. 44, 56 (1991) ("[A] jurisdiction that provides judicial determinations of probable cause within 48 hours of arrest will, as a general matter, comply with the promptness requirement of [the Fourth Amendment].").

117. *Cf.* United States v. Sharpe, 470 U.S. 675, 687–88 (1985) (finding a twenty-minute stop reasonable when the suspect was responsible for some of the delay); *see also* AM. LAW INST., MODEL CODE OF PRE-ARRAIGNMENT PROCEDURE § 110.2(1) (1975) (permitting stops of up to twenty minutes).

118. *See* AM. BAR ASS'N, STANDARDS GOVERNING TECHNOLOGICALLY-ASSISTED PHYSICAL SURVEILLANCE Std. 2-9.2 (2012) [hereinafter ABA STANDARDS ON PHYSICAL SURVEILLANCE], *available at* http://www.americanbar.org/publications/criminal_justice_section_archive/crimjust_ standards_taps_blk.html (defining "legitimate law enforcement objective" as "detection, investigation, deterrence or prevention of crime, or apprehension and prosecution of a suspected criminal").

119. Kerr, *supra* note 16 (manuscript at 24).

120. *See Sharpe*, 470 U.S. at 687–88; Florida v. Royer, 460 U.S. 491, 500 (1983) (stating that "an investigative detention [on less than probable cause] must be temporary and last no longer than is necessary to effectuate the purpose of the stop" and holding a fifteen-minute detention in a small room to be the functional equivalent of arrest).

121. I have used the term "virtual searches" to refer to searches that do not require physical intrusion. *See* Slobogin, *supra* note 30, at 12.

Other approaches to regulation of physical surveillance in public have been proposed, but they face very significant administrability problems. For instance, Professor Susan Freiwald has answered the search question in terms of the extent to which the surveillance is hidden, intrusive, continuous, and indiscriminate.[122] While figuring out whether a police action is hidden or indiscriminate is relatively simple, the intrusiveness inquiry, as Professor Freiwald admits, "requires a judgment about levels of intrusiveness" and an assessment of "the richness of the information acquired."[123] She also provides no useful definition of "continuous."[124] Much more elaboration is needed if police and courts are to have any idea whether a particular investigative action is regulated. A similar comment can be made about a proposal from Mark Blitz that would regulate surveillance "that has the capacity to systematically track, or otherwise collect private information about [an] individual's movements or other activities in ways that go meaningfully beyond the surveillance that is possible with unaided observation."[125] This definition leaves unanswered what "private information" is and when surveillance goes "meaningfully beyond" unaided observation (which in any event, as noted below, can be at least as intrusive as technologically-aided observation).

Rules based on duration are easier to understand and abide by. While precise time divisions such as those used in this provision are arbitrary in the sense that they apply regardless of how intrusive the search actually is, time limitations as a method of defining constitutional protections have a solid pedigree. The forty-eight-hour period that defines when an arrestee must be taken to a magistrate, referenced above, is one example. While the Supreme Court has not been as rigid about when a stop becomes an arrest, its case law on the subject also leans heavily on the durational element.[126] A third

122. Susan Freiwald, First Principles of Communications Privacy, 2007 STAN. TECH. L. REV. 3, ¶ 50 (2007), *available at* http://stlr.stanford.edu/pdf/freiwald-first-principles.pdf.

123. *Id.* at ¶¶ 64–65.

124. *See id.* at ¶¶ 69–70 (discussing continuous investigations and suggesting that tapping an individual's e-mail communications for three months is clearly continuous).

125. Mark Blitz, United States v. Jones—*and the Forms of Surveillance that May Be Left Unregulated in a Free Society*, USVJONES.COM (June 4, 2012), http://usvjones.com/2012/06/04/united-states-v-jones-and-the-forms-of-surveillance-that-may-be-left-unregulated-in-a-free-society.

126. *See* INS v. Delgado, 466 U.S. 210, 224 (1984) (finding that no seizure occurred where the confrontation lasted less than five minutes, and pointing out that the secondary checkpoints in United States v. Martinez-Fuerte, 428 U.S 543 (1976), where the Court held that a seizure had

example of a time-limited constitutional rule, from outside the search and seizure context, is the Court's holding that two weeks marks the point at which police may reinitiate interrogation of a suspect who has asserted his right to counsel, even though the degree of coercion experienced by suspects can vary significantly over time depending upon a wide variety of circumstances.[127] These types of prophylactic standards are a well-established method of construing many of the clauses in the Constitution, in recognition of the institutional limitations on rulemaking.[128] Congress has also relied on time periods as a means of distinguishing regulatory thresholds in the surveillance context.[129]

Note three other aspects of the provision. First, this provision applies to naked-eye observation as well as technologically-aided surveillance. Overt surveillance by the police can be just as intrusive as covert tracking or monitoring.[130] Second, given the definition of "targeted" search, this provision applies not only to observation of suspicious people but also to targeted surveillance of places. Under this provision, government would need at least reasonable suspicion for targeted surveillance of a particular place that lasts longer than twenty minutes and probable cause when such surveillance exceeds forty-eight hours (with a new probable cause finding required after thirty days). Third, no court order is required for short-term public searches or when exigency exists. Thus, for instance, if an officer legitimately stationed on a street corner observes suspicious activity that, over a twenty-minute period, develops into reasonable suspicion that requires the officer to follow the suspect, a court order would not be necessary to continue the pursuit. Given the fast-moving nature of

---

occurred, lasted up to five minutes).

127. *See* Maryland v. Shatzer, 130 S. Ct. 1213, 1223 (2010) ("14 days . . . provides plenty of time for the suspect to get reacclimated to his normal life, to consult with friends and counsel, and to shake off any residual coercive effects of his prior custody.").

128. *See* David A. Strauss, *The Ubiquity of Prophylactic Rules*, 55 U. CHI L. REV. 190, 208 (1988) ("Under any plausible approach to constitutional interpretation, the courts must be authorized—indeed, required—to consider their own, and the other branches', limitations and propensities when they construct doctrine to govern future cases.").

129. *See, e.g.*, Electronic Communications Privacy Act, 18 U.S.C.A. § 2518(5) (West 2012) (limiting electronic surveillance warrant to thirty days); *id.* at § 2703 (requiring a warrant for acquiring information in electronic storage for less than 180 days and only a subpoena for access to information in storage over 180 days).

130. *See* Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 277 (2002) (reporting a study in which participants ranked overt police observation of a person on the street to be as "intrusive" as overt camera surveillance and more intrusive than a fifteen-second roadblock stop).

most street surveillance, the exigency exception would presumably apply very frequently in this setting.

(2) Targeted Data Searches

(a) A targeted data search of data held by an institutional third party that accumulates information about activities or transactions that take place over more than a 48-hour period requires probable cause, and a warrant unless exigent circumstances exist.

(b) A targeted data search of data held by an institutional third party that is not governed by (2)(a) requires reasonable suspicion, and a court order unless exigent circumstances exist.

Commentary: The commentary to Part II(1) explains the rationale for the forty-eight-hour cut-off in this provision. Under this provision, only reasonable suspicion would be required to obtain phone or internet service provider logs detailing communications made by the target at a particular point in time. But probable cause would be required if the government sought data on calls made over more than a two-day period, a monthly bank record or credit card statement, or a medical record that describes symptom history.

Another approach to targeted data searches that would be consistent with proportionality reasoning would be to focus on the privacy interest associated with the type of record being accessed.[131] Under this scheme, accessing medical records might require probable cause, whereas phone records might be accessible on something less. Either regulatory scheme is somewhat arbitrary and over- and under-inclusive in terms of accurately capturing relative intrusiveness. The proposed provision is more pragmatic, however, for reasons similar to those noted in connection with public searches. Differentiating the relative privacy interest in the various types and subtypes of records that law enforcement might seek (for instance, medical, bank, credit card, travel, phone, utility, real estate records) is a difficult chore that will inhibit the creation of clear rules.[132] Furthermore, some records

131. This is the approach I took in PRIVACY AT RISK. *See* SLOBOGIN, *supra* note 54, at 180–96.

132. For instance, the American Bar Association's effort in this regard, in which I was involved, resulted in provisions that create four different types of institutional third party records ("highly private," "moderately private," "minimally private," and "not private")

searches, such as those that occur in connection with data-mining, might access more than one type of record, and investigators cannot always know ahead of time the type of record they will be accessing.[133]

This provision rejects the third party doctrine, but only if the third party is an "institution" (a commercial enterprise or government agency). Thus, this provision does not apply to efforts at obtaining data from a non-institutional third party, such as a friend of the target. In these situations, the Supreme Court has held that the Fourth Amendment does not apply.[134] Even though this type of data acquisition would be a search under these provisions, the fact that a person, as opposed to an impersonal entity, has an autonomy interest in controlling information in his or her possession may require different treatment than when the third party is an institution.[135]

This provision is also inapposite when data is sought from the target, whether the target is a person or an institution. In *United States v. Hubbell*,[136] the Supreme Court held that when the records are in the possession of the person who is the focus of the investigation rather than a third party, a subpoena forcing production of the records will often be insufficient, and a warrant may be required for reasons having to do with the Self-Incrimination Clause of the Fifth Amendment.[137] Further, because of this statute's definition of "search"

---

depending on application of four criteria: (1) the extent to which the transfer of the information to a third party "is necessary to participate meaningfully in society or in commerce, or is socially beneficial, including to freedom of speech and association;" (2) the extent to which the information is "personal," "likely to cause embarrassment or stigma if disclosed," and otherwise would not be revealed outside "one's close social network;" (3) the extent to which the information is accessible by persons other than the institutional third party; and (4) the extent to which "existing law, including the law of privilege," allows access to the information. AM. BAR ASS'N, STANDARDS ON LAW ENFORCEMENT ACCESS TO THIRD PARTY RECORDS Stds. 25-4.1, 25-4.2 (2012) [hereinafter ABA STANDARDS ON THIRD PARTY RECORDS], *available at* http://www.americanbar.org/groups/criminal_justice/policy/standards/law_enforcement_access.html.

133. Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 583–84 (2009) (noting that police "will necessarily collect information at the end of its dissemination, whereas judgments as to whether and when privacy is likely must be made prospectively" and "[a]s a result, the Fourth Amendment rules that the police must apply ex ante must hinge on details of the history of information that they cannot know ex ante").

134. Hoffa v. United States, 385 U.S. 293, 302 (1966) (holding that the Fourth Amendment does not protect "a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it").

135. *See* SLOBOGIN, *supra* note 54, at 160 ("[E]ven if . . . one accepts the 'social undercover agent' cases as valid law, they are distinguishable from the 'institutional undercover agent' cases like *Miller* because social agents have an autonomy interest that institutional agents lack.").

136. 530 U.S. 27 (2000).

137. *Id.* at 44–45 (holding that the Fifth Amendment requires the government to show it

(which speaks of obtaining information about a "person or place"), this provision does not regulate data searches when the target is a commercial enterprise or government agency. This situation is governed by cases like *United States v. Morton Salt Co.*,[138] which hold that when the focus of an investigation is a business entity, mere "official curiosity" might be sufficient grounds for obtaining records.[139] This approach is consistent with proportionality reasoning if one assumes that institutional entities have a much reduced privacy interest.[140]

(3) General Public and Data Searches

(a) Public or data searches that are general in nature must be authorized by legislation or regulations issued pursuant to such legislation and may focus on a discrete group only if the group has meaningful access to the legislative or administrative process.

(b) Rules governing access to, storage of, and analysis of information obtained in a general search must apply evenly or randomly to all members of the group, unless the requirements of II(1) or (2) are met.

Commentary: This provision regulates searches that do not have a specific person or place as a target, but rather are aimed at observing or gathering information about large numbers of people, in the hope that crime will be detected or deterred. Under the Supreme Court's third party doctrine, general public and data searches are not governed by the Fourth Amendment unless a physical trespass is somehow involved.[141] If the Court were to hold that these types of governmental actions were searches, it would probably turn to its "special needs" analysis which, as noted above,[142] would require

---

has "prior knowledge" of the "existence and authenticity" of the specific documents it seeks to subpoena from the person who possesses the documents).

138. 338 U.S. 632 (1950).

139. *See id.* at 652 ("Even if one were to regard the request for information in this case as caused by nothing more than official curiosity, nevertheless lawenforcing [sic] agencies have a legitimate right to satisfy themselves that corporate behavior is consistent with the law and the public interest.").

140. *See* FCC v. AT&T, Inc., 131 S. Ct. 1177, 1185 (2011) ("The protection in FOIA against disclosure of law enforcement information on the ground that it would constitute an unwarranted invasion of personal privacy does not extend to corporations.").

141. *See supra* text accompanying notes 27–30.

142. *See supra* text accompanying notes 79–80.

individualized suspicion if the "primary purpose" of the general search is a "general interest in crime control," but otherwise would grant deference to the government's program. As applied, outcomes under this test are difficult to predict. Checkpoints to nab drunk drivers or to detect illegal immigrants at some distance from the border are permissible,[143] but a roadblock set up to detect narcotics is not;[144] a drug testing program aimed at students in extracurricular activities is permissible,[145] but a drug testing program for pregnant mothers is not.[146]

This provision instead applies political process theory to general searches.[147] It imposes three requirements on general search programs. First, they must be approved or authorized by a legislature. Many of the Court's special needs cases involve general searches implemented by the executive branch, with no legislative input.[148] Second, the group affected by the general search must have meaningful access to the legislative process. Admittedly, much rides on the word "meaningful." One measure of this concept, noted earlier, would be the extent to which the general search will affect members of the legislature. As Justice Jackson stated, "there is no more effective practical guaranty against arbitrary and unreasonable government than to require that the principles of law which officials would impose upon a minority must be imposed generally."[149] Third, consistent with this view, the group search, both as authorized and as implemented, must affect everyone within the group equally. If instead persons or places are singled out, then the provisions regarding targeted searches are triggered.

---

143. *See generally* Mich. Dep't State Police v. Sitz, 496 U.S. 444 (1990) (upholding a sobriety checkpoint); United States v. Martinez-Fuerte, 428 U.S. 543 (1976) (upholding a roadblock to detect illegal immigrants sixty-six miles north of the border).

144. City of Indianapolis v. Edmond, 531 U.S. 32, 37–38 (2000) (holding unconstitutional a checkpoint set up to detect narcotics in vehicles, and trying to distinguish this holding from *Martinez-Fuerte* and *Sitz*).

145. *See* Bd. of Educ. v. Earls, 536 U.S. 822, 836 (2002) (upholding drug testing program for students in extracurricular activities).

146. Ferguson v. City of Charleston, 532 U.S. 67, 79–80 (2001) (invalidating testing program for pregnant mothers and trying to distinguish this holding from Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646 (1995), which upheld a drug testing program for student athletes).

147. *See generally* Richard C. Worf, *The Case for Rational Basis Review of General Suspicionless Searches and Seizures*, 23 TOURO L. REV. 93 (2007) (applying, for the first time, political process theory to general searches).

148. *See* Slobogin, *supra* note 83, at 133–34 (describing the Court's special needs cases).

149. Ry. Express Agency, Inc. v. New York, 336 U.S. 106, 112 (1949) (Jackson, J., concurring).

Thus, for instance, a drone or camera surveillance system would be permissible under this provision only if the relevant municipal government approved it and the system covered the entire municipality or rotated its focus on a random or neutral basis. If instead the drones or cameras were programmed to monitor particular areas, reasonable suspicion or probable cause, depending upon the length of the surveillance, would be required. Rather than "individualized suspicion," the justification in such cases could be based on statistical analysis of crime within the area. As another example, a data-mining program run by the federal government that will access monthly records would have to be authorized by Congress and would need to apply to the entire country unless algorithms can produce, within a subset of targets, evidence of crime against fifty percent of that subset during the time of the warrant.[150]

V. OTHER POSSIBLE PROVISIONS

A statute or regulation that comprehensively regulates public and data searches would also contain provisions covering a number of other important issues. These provisions would deal with post-search implementation matters such as whether and when notice of the search is required, how long and under what conditions information obtained during the search may be maintained, and the circumstances under which this information may be disclosed. Provisions must also address accountability issues, including remedies. The following discussion briefly comments on these two general categories, relying in large part on work done by the American Bar Association's Criminal Justice Section.

A. Post-Search Regulation

In the traditional search case, the target knows that a search of his or her house, person, papers, or effects has occurred. Where searches are covert—often the case when government uses technology—notice of a more formal nature might be constitutionally required.[151] In any event, notice is a useful way of ensuring accountability because officials will know that their targets will eventually find out about the surveillance. Thus, the ABA Standards on Law Enforcement Access to

150. For further elaboration, see Slobogin, *supra* note 83, at 138–41.

151. *See* Berger v. New York, 388 U.S. 41, 60 (1967) (suggesting that post-surveillance notice is constitutionally required in the electronic surveillance context).

Third Party Records require notice to the target of a records search within thirty days of its occurrence unless the records are only "minimally protected."[152] The notice can be delayed if harm to public safety or the investigation would result, but may only be dispensed with entirely "where it would be unduly burdensome given the number of persons who must otherwise be notified, taking into consideration, however, that the greater number of persons indicates a greater intrusion into privacy."[153]

The Supreme Court has suggested, without deciding, that the Due Process Clause requires law enforcement to keep a tight rein on information it accumulates.[154] The information obtained through public and data searches can be voluminous and highly personal, so the duty to prevent leaks, hacking, and dissemination to inappropriate persons is particularly strong in this context. The ABA's Standards on Third Party Records contain a number of provisions governing these matters. For instance, the standards require that records be kept "reasonably secure from unauthorized access,"[155] that all attempted and successful access to records that are moderately or highly protected be subject to audit,[156] and that records be "destroyed according to an established schedule."[157] An example of this type of schedule in the physical surveillance setting comes from Washington, D.C., where footage from surveillance cameras is destroyed after ten days unless needed for evidence or training purposes.[158]

The ABA's standards also impose limitations on the disclosure of information obtained in data searches. In essence, the standards state that disclosure may occur only in connection with criminal investigation and training or if necessary to protect the public.[159] Other disclosures must be specifically authorized by law.[160]

---

152. ABA STANDARDS ON THIRD PARTY RECORDS, *supra* note 132, Std. 25-5.7(a).

153. *Id.* Std. 25-5.7(f).

154. *See* Whalen v. Roe, 429 U.S. 589, 605 (1977) ("The right to collect and use . . . data for public purposes . . . in some circumstances . . . arguably has its roots in the Constitution . . . .").

155. ABA STANDARDS ON THIRD PARTY RECORDS, *supra* note 132, Std. 25-6.1(a)(i).

156. *Id.* Std. 25-6.1(b)(i).

157. *Id.* Std. 25-6.1(b)(ii).

158. NANCY G. LA VIGNE ET AL., URBAN INST., EVALUATING THE USE OF PUBLIC SURVEILLANCE CAMERAS FOR CRIME CONTROL AND PREVENTION 76 (2011), *available at* http:// www.urban.org/UploadedPDF/412403-Evaluating-the-Use-of-Public-Surveillance-Cameras-for-Crime-Control-and-Prevention.pdf.

159. ABA STANDARDS ON THIRD PARTY RECORDS, *supra* note 132, Std. 25-6.2.

160. *Id.* Std. 25-6.2(e). Some have argued that, if these types of disclosure rules exist, rules limiting access to information are not necessary. *E.g.*, William J. Stuntz, *Local Policing After the Terror*, 111 YALE L.J. 2137, 2183–84 (2002). I take issue with that conclusion in SLOBOGIN,

B. Accountability

Accountability can be accomplished through a number of mechanisms. Already noted is the role notice and auditing can play. The ABA Standards on Technologically-Assisted Physical Surveillance also require the creation of "administrative rules which ensure that the information necessary for . . . accountability exists."[161] In short, some method of "watching the watchers"[162] should be established. As another means of controlling discretion, the standards require that law enforcement agencies conduct "periodic review . . . of the scope and effectiveness of technologically-assisted physical surveillance" and that the agencies "[m]aintain[] and [make] available to the public general information about the type or types of surveillance being used and the frequency of their use."[163]

As to sanctions that might be imposed for violation of the rules, administrative punishment, damages, injunctions, and criminal prosecution can all be on the table, in addition to the traditional Fourth Amendment remedy of exclusion. I have expressed a preference for a damages action over exclusion even in the traditional search context.[164] Some sort of alternative to exclusion—a remedy that applies only in criminal cases—is even more important where technology allows government to access information about thousands of innocent people who will never have the option of invoking the rule.[165] Furthermore, the exclusion remedy is a poor fit for violation of

---

supra note 54, at 13–32, 199–201.

161. ABA STANDARDS ON PHYSICAL SURVEILLANCE, *supra* note 118, Std. 2-9.1(f)(i).

162. DAVID BRIN, THE TRANSPARENT SOCIETY: WILL TECHNOLOGY FORCE US TO CHOOSE BETWEEN PRIVACY AND FREEDOM? 334 (1998) (arguing that the only way for people to confront governmental surveillance efforts is to watch those watching them).

163. ABA STANDARDS ON PHYSICAL SURVEILLANCE, *supra* note 118, Stds. 2-9.1(f)(iv), (v).

164. *See generally* Christopher Slobogin, *Why Liberals Should Chuck the Exclusionary Rule*, 1999 ILL. L. REV. 363 (discussing a damages alternative to exclusion). However, I have also argued that, as a method of deterring pretextual use of general public and data searches, evidence found during such a search that is not related to its purpose (e.g., cocaine found during a terrorist-prevention surveillance program) could be excluded. Slobogin, *supra* note 83, at 142–43.

165. Another issue not addressed by the proposed statute is standing to challenge a public or data search. *See* Kerr, *supra* note 16 (manuscript at 33–34) (arguing that because mosaic searches might affect many people to different degrees, determining who has standing will be "difficult"). Under the Court's current jurisprudence, only the person whose own privacy interests have been intruded upon has standing. *See* Rakas v. Illinois, 439 U.S. 128, 143 (1978) (stating that Fourth Amendment standing depends upon whether the individual has a "legitimate expectation of privacy in the invaded place"). Under that standing rule for invoking

post-search rules, like those dealing with notice and dissemination, that do not involve illegal access to excludable information.[166]

VI. CONCLUSION

The statute proposed in this article attempts to implement mosaic theory through application of two frames for thinking about the Fourth Amendment: the proportionality principle and political process theory. It answers the four questions left open after *Jones* as follows:

1. Differentiating between short-term and long-term physical surveillance can be justified under proportionality analysis, and clear, if somewhat arbitrary, distinctions based on the duration of the surveillance can be established.
2. Physical surveillance (including, but not limited to, tracking) should not always require probable cause. Proportionality analysis suggests that reasonable suspicion or an even lower standard is an adequate justification for government actions that are only moderately or minimally intrusive.
3. The nature of the offense should normally not affect the justification required by proportionality reasoning. The one exception occurs when a search is necessary to prevent a serious, specific threat.
4. Proportionality reasoning should also apply when government engages in institutional data searches. The third party doctrine should be discarded in this situation; instead, justification should be required for data access, but should vary depending upon the length of time over which the sought-after transactions occurred.

The statute also addresses a number of questions not raised in *Jones*. It redefines search for Fourth Amendment purposes to

---

exclusion or seeking damages, in practical effect there would be no remedy for public and data searches of third parties. The preferable standing rule, arguably required when the goal of a constitutional rule is deterrence, is target or universal standing. *See* Arnold Loewy, *Police-Obtained Evidence and the Constitution: Distinguishing Unconstitutionally Obtained Evidence from Unconstitutionally Used Evidence*, 87 MICH. L. REV. 907, 939 (1989) ("[W]hen obtaining evidence is the constitutional wrong, [the proposed remedy] should be subjected to a cost/benefit analysis. If allowing third-party standing would deter the objectionable practice, such standing should be permitted.").

166. SLOBOGIN, *supra* note 54, at 133–34.

conform to its lay meaning. It defines probable cause and reasonable suspicion more definitively than the case law does by providing that probable cause searches must be likely to obtain significant evidence of wrongdoing, while permitting reasonable suspicion searches that are likely to discover leads to such evidence. It also introduces the idea that general searches—searches of groups in the absence of suspicion—should be regulated differently than targeted searches, through reliance on political process theory.

As important as the content of these proposals is the method of explicating them. Construction of statutes regulating government investigation is crucial for a number of reasons. First, implementation of Fourth Amendment theory through statutory provisions requires confrontation with the implications of that theory. Until theoreticians are forced to put their prescriptions into action, the logic and feasibility of their proposals cannot be fully evaluated. Second, by providing a template for legislatures, a statutory proposal increases the probability that legislatures will get involved in the process of regulating searches, which itself has several advantages. As Justice Alito suggested in *Jones*, legislatures are better equipped than courts, bound as they are by the case and controversy requirement and judicial restraint, to provide detailed and comprehensive regulations about a wide range of scenarios.[167] And courts can do a much more competent job evaluating the constitutionality of a given practice if a statute provides them with the framework in which it occurs.[168] For instance, courts might think quite differently about justification requirements if they know that the government is constrained by rules governing notice, disclosure, and accountability.

Another possible advantage that legislation has over judicial analysis, also raised by Justice Alito, is that legislatures can be more

---

167. *See* United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring) ("A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way."); *see also* Craig M. Bradley, *Criminal Procedure in the "Land of Oz": Lessons for America*, 81 J. CRIM. L. & CRIMINOLOGY 99, 129 (1990) ("Since Supreme Court rulemaking is limited by the Court's docket, the facts of the cases before it, and its frequent unwillingness to 'mandate a code of behavior for state officials,' the result is patchwork of rules that cover some, but ignore equally important aspects of criminal procedure." (quoting Moran v. Burbine, 475 U.S. 412, 425 (1986))).

168. *See* Anthony G. Amsterdam, *The Supreme Court and the Rights of Suspects in Criminal Cases*, 45 N.Y.U. L. REV. 785, 791 (1970) (Without a statute, "[t]he Court cannot know whether the conduct before it is . . . unconnected or connected with a set of other practices or . . . the comprehensive shape of the set of practices involved, . . . their relations, their justifications, their consequences.").

responsive than courts to changes in the technology used to carry out searches.[169] If the proposed statute is adopted, however, this advantage would be muted, because regulation would not be driven by the method of investigation. A search would occur whenever government is looking for evidence of wrongdoing, regardless of how it does so, and justification levels would be set according to the duration of the search, not the type of technology used or the type of information sought. This approach is not only consistent with the Fourth Amendment's language and history, but should be able to accommodate even significant changes in the way government chooses to investigate its citizens.

169. *See Jones*, 132 S. Ct. at 964 (Alito, J., concurring) ("In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative."); *see also* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 806 (2004) ("Technological change may reveal the institutional limits of the modern enterprise of constitutional criminal procedure, exposing the need for statutory guidance when technology is changing rapidly.").