NOTE

Privacy Is the Problem: *United States v. Maynard* and a Case for a New Regulatory Model for Police Surveillance

*Matthew Radler**

ABSTRACT

Inescapably, the debate in the United States about law enforcement's use of electronic surveillance is defined in terms of privacy. Whether discussed by courts, commentators, or legislators, the principal and often the only justification put forth for regulating the use of a given technology by the police is that it invades an interest somehow described as private. But as surveillance technology has extended to conduct that takes place on public property and in plain view of society at large, this rationale for regulation has become incapable of justifying the rules that result. This demand for privacy-based rules about public-conduct surveillance reached its apex (thus far) in 2010 in United States v. Maynard, *the appellate decision affirmed on other grounds by the Supreme Court's property-based ruling in* United States v. Jones. Maynard*'s theory of privacy rights in the context of police use of tracking devices—that they are violated by the mere aggregation of data—is so vulnerable to circumvention by police agencies that its efficacy as a basis for regulation is questionable at best. This Note proposes an alternative rationale for*

* J.D., May 2012, The George Washington University Law School; B.S.J., 2009, Northwestern University. Thank you to Professor Paul Butler for comments on the initial direction of this Note's thesis and research; to the staff of *The George Washington Law Review*, particularly Richard Crudo, Ben Kapnik, Lauren Miller Forbes, Sean Sherman, Will McAuliffe, Timothy Li, Nicole Durkin, and Charles H. Davis for their edits, comments, observations, and time; and last but certainly not least, to Aubrey McCullen for her insight as an independent reader and my most forgiving critic.

regulation of public-conduct surveillance, as well as a theory of institutional harm and an alternative rulemaking authority—an administrative agency—to address public-conduct surveillance issues.

In an era when police action is the primary determinant of who is convicted of crimes, without meaningful review via trial, unchecked surveillance renders the judiciary a rubber stamp for local executive power; the demand for an ex ante record restores the supervisory role of the courts over police conduct. Preserving that institutional role, instead of protecting an increasingly difficult-to-justify notion of individual privacy in public behavior, provides a durable rationale, and ensuring that it is given full effect will require administrative, rather than judicial or legislative, oversight.

TABLE OF CONTENTS

INTRODUCTION

In its January 2012 decision in *United States v. Jones*,[1] the Supreme Court unanimously concluded that law enforcement's attachment of a tracking device to a citizen's property triggers the application of the Fourth Amendment.[2] Yet in terms of surveillance law, the majority opinion expressly avoided the larger issue of whether monitoring of public conduct, without physical intrusion upon or interaction with property, constitutes a "search" and thus falls within the Amendment's regulation of "searches and seizures."[3]

After *Jones*, the question of monitoring without trespass—e.g., the aggregation of data using technologies such as tracking a fixed device already installed in a vehicle,[4] the retrieval of location records from cellular phone service providers,[5] or even the use of aerial unmanned drones equipped with cameras[6]—remains an open one. The

1 United States v. Jones, 132 S. Ct. 945 (2012).

2 *Id.* at 953–54.

3 *See id.*

4 *See generally Stolen Vehicle Slowdown & Assistance*, ONSTAR, http://www.onstar.com/web/portal/securityexplore?tab=1 (last visited Mar. 31, 2012) (describing how technology installed in your vehicle can permit a third-party service to track its location in the event of theft).

5 *See In re* Application of United States for an Order Directing A Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 308–09 (3d Cir. 2010) (discussing the government's pursuit of location data from phone companies who retain records of where users place and receive telephone calls).

6 *See* Dan Gunderson, *Unmanned Aircraft a Controversial Surveillance Tool for N.D. Law Enforcement*, MINN. PUB. RADIO (Jan. 31, 2012), http://minnesota.publicradio.org/display/web/2012/01/30/unmanned-aircraft-police/.

conduct being tracked is public in that it occurs in public places, but the entire debate about this form of surveillance has fallen into a familiar pattern: conflicting theories of privacy rights.[7]

This has proven to be the case for public officials, such as Senator Ron Wyden of Oregon, who termed location tracking using citizens' cellular phones a "fairly serious intrusion of privacy comparable to searching their house or tapping their phone calls."[8] Privacy has also been the dominant issue of concern for scholars on the subject,[9] as well as a host of student commentators.[10] Casting discussions about novel surveillance technologies in terms of individual privacy rights and the Constitution is a common theme in scholarly legal debate[11]—and that debate draws much of its theoretical support from judicial interpretations of the Fourth Amendment.[12] The notion that privacy theories are the natural basis for defining what types of surveillance should or should not be regulated thus goes largely unchallenged. This Note examines the costs associated with these privacy-based approaches to the monitoring without trespass question left unresolved by *Jones*, and proposes an alternative doctrinal basis for regulating this form of surveillance: not regulating monitoring without trespass would threaten institutional, particularly judicial, power.

At present, there is no uniform legal framework for assessing the legality of public-conduct monitoring without a physical trespass. The majority of federal courts that have taken up the monitoring issue found no constitutional argument for regulating the aggregation of

---

7 *See* Haley Plourde-Cole, Note, *Back to* Katz*: Reasonable Expectation of Privacy in the Facebook Age*, 38 FORDHAM URB. L.J. 571, 577 (2010) (arguing that such tactics should be governed by a warrant requirement because they implicate a privacy interest).

8 Jason Chaney, *Wyden Seeks New Legislation for GPS, Cell Phone Tracking*, CENT. OREGONIAN (Feb. 21, 2011), http://www.centraloregonian.com/archives/story.aspx/12111/wyden-seeks-new-legislation-for-gps-cell-phone-tracking.

9 *See, e.g.*, Bennett L. Gershman, *Privacy Revisited: GPS Tracking as Search and Seizure*, 30 PACE L. REV. 927 (2010); Renée McDonald Hutchins*, Tied Up in* Knotts*? GPS Technology and the Fourth Amendment*, 55 UCLA L. REV. 409 (2007).

10 *See, e.g.*, Oleg Kobelev, Recent Development, *Big Brother on a Tiny Chip: Ushering in the Age of Global Surveillance Through the Use of Radio Frequency Identification Technology and the Need for Legislative Response*, 6 N.C. J. L. & TECH. 325 (2005); Aaron Renenger, Note, *Satellite Tracking and the Right to Privacy*, 53 HASTINGS L.J. 549 (2002).

11 *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 802 n.7 (2004) (surveying a broad cross-section of legal theorists and finding a consensus about the Fourth Amendment as the key means for protecting privacy and limiting government action).

12 Beginning with Justice Harlan's concurrence in *Katz v. United States*, 389 U.S. 347, 360–62 (1967), the Fourth Amendment's applicability to a given law enforcement tactic has come to be anchored in an analysis of whether that tactic intrudes upon a citizen's privacy interests. For a fuller explanation of this standard, see *infra* Part III.

data from citizens' travel or public behavior,[13] taking a narrower view of what is or is not "private" in American life.[14] With its emphasis on property-based rules, *Jones* leaves this approach intact.

These arguments about the Constitution, privacy rights, and the need for regulating police surveillance came into sharper focus in 2010 and 2011: first, in 2010, with the D.C. Circuit's decision in *United States v. Maynard*,[15] which the *Jones* Court affirmed on property-based grounds, and second, in 2011, with Senator Wyden's proposed legislation to subsume the entire spectrum of location surveillance within a one-size-fits-all warrant regime.[16] *Maynard*, unlike *Jones*, brought tracking technologies under the Fourth Amendment by relying on an expansive theory of privacy rights.[17] The central tenet of this approach is that comprehensive public surveillance violates a privacy interest because of the amount of information that is gathered.[18] But as this Note argues, *Maynard* demonstrates that a regulatory approach to surveillance technologies[19] based on expansive privacy theories is part of the ongoing problem, not the solution. By contrast, the proposed legislation, the Geolocational Privacy Surveillance Act ("GPS Act"),[20] cuts too broadly, reducing investigative efficiency by requiring a warrant even when no current definition of private information would be implicated.[21]

The uncertain character of privacy interests in public conduct—the interests that *Maynard* identified and that the *Jones* majority

---

13 *See, e.g.*, United States v. Pineda-Moreno, 591 F.3d 1212, 1215–17 (9th Cir. 2010), *vacated*, No. 10-7515 (U.S. Feb. 21, 2012); United States v. Garcia, 474 F.3d 994, 998 (7th Cir. 2007); United States v. Burton, 698 F. Supp. 2d 1303, 1307–08 (N.D. Fla. 2010).

14 For a fuller discussion of the majority view among the federal appellate courts and their rejection of a more expansive conception of privacy interests, see *infra* Part III.A.

15 United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010), *aff'd on other grounds sub nom.* United States v. Jones, 132 S. Ct. 945 (2012).

16 Geolocational Privacy and Surveillance (GPS) Act, S. 1212, 112th Cong. (2011).

17 *Maynard*, 615 F.3d at 561–65.

18 For more details on *Maynard's* holding, see *infra* Part III.B.

19 GPS is by no means the only technology developed or currently in use that reveals a target's location. Commentators have noted new technologies ranging from the analysis of cellular-site data, turned over to the government by third parties, to chips that reveal location information through radio frequency data, to unmanned aerial drones. *See, e.g.*, Troy Roberts, *On the Radar: Government Unmanned Aerial Vehicles and Their Effect on Public Privacy Interests from Fourth Amendment Jurisprudence and Legislative Policy Perspectives*, 49 JURIMETRICS J. 491, 492 (2009); Renenger, *supra* note 10, at 551–52. The legal issues regarding public surveillance and controlling police behavior presented in *Maynard* are not technology-specific and are implicated as long as a given tactic involves surreptitiously tracking a citizen and recording his or her public movements.

20 GPS Act, S. 1212, 112th Cong. (2011).

21 *See id.*

avoided[22]—results in a standard that allows the police to respond strategically to circumvent and weaken judicial rules.[23] This Note argues that a theory of institutional harm—one that considers the corrosive effect of unregulated surveillance on the judiciary's power to check arbitrary executive behavior—provides a sounder rationale for regulating public-conduct surveillance technologies than does a privacy theory.[24]

Outside of the criminal procedure realm, federal administrative law is another area of scholarship where agency discretion, the need for a contemporaneous record justifying action taken against private parties, and judicial review have long been topics of discussion.[25] This scholarship provides a key insight: that if one thinks of police departments as administrative agencies, many of those police departments' actions directed at private citizens are done without a meaningful ex ante record, thereby grossly limiting judicial review of the underlying rationale for investigative decisions.[26] The warrant requirement cures this institutional imbalance of power by forcing police agencies to generate a presurveillance explanation for why a particular citizen is a target.

Ultimately, balanced regulation of law enforcement surveillance activity will require a form of administrative rulemaking, rather than judicial or purely legislative action. This Note proposes that a conditional grant program that imposes a regulation-based warrant requirement would make law enforcement agencies more effective and would prevent institutional harm. Such an approach could recreate many of the most useful features of existing surveillance law, such as exclusion of evidence obtained without a court order,[27] while also ensuring more nuanced and timely regulation of surveillance tactics as they appear. For example, such an agency would be compelled to respond to petitions for rulemaking, giving citizen groups and law enforcement organizations an arena in which to demand that new issues be addressed.[28]

Part I of this Note examines salient traits of local law enforcement agencies, as well as how these agencies use GPS tactics. Part II

---

22 *See* United States v. Jones, 132 S. Ct. 945, 954 (2012) ("It may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question.").

23 *See infra* Part II.

24 *See infra* Part V.

25 *See infra* Part V.A.

26 *See infra* Part V.A.

27 *See infra* Part VI.A–B.

28 *See infra* Part VI.A.

details how police agencies circumvent or weaken judicial rules when standards are unclear or allow for justifications after a tactic is employed. Part III analyzes *United States v. Maynard* and how its novel, privacy-centered approach survives the *Jones* decision and presents the regulatory defects identified in Part II. Part IV examines the flaws in both the legislative approach before 2010 and the proposed GPS Act. Part V proposes a theory of harm beyond the popular focus on privacy: that by analogizing to doctrinal arguments found in administrative law, the real problem with unregulated surveillance is its corrosive effect on judicial power. Part VI proposes a solution that uses an administrative law framework and relies on Congress's conditional spending power and the close financial relationship between the federal government and local police agencies. The solution would require an agency delegated the task—a Surveillance Technology Review Board—to set warrant standards for different technologies, to be accountable to public demands for rulemaking, and to address emerging issues more quickly and with more nuance than Congress and more effectively than the courts.

I. Police Agencies and Public-Conduct Surveillance: Tactics and Traits

When judges and scholars talk about using the Fourth Amendment to limit government use of surveillance technologies, they are by definition talking about the activities of thousands of local police departments. By one estimate, municipal, county, and state law enforcement officers and their support staff outnumber federal agents seven to one.[29] If the Fourth Amendment, including the privacy and property theories ascribed to it, is intended to regulate surveillance by the local police, it is useful to consider the emerging traits of this institution and how it employs these novel surveillance technologies.

As a threshold matter, any effort to uniformly regulate the police must confront the diverse character of this institution. The United States features more than 15,000 discrete state and local law enforcement agencies, ranging from rural departments with a few sworn officers to major municipal organizations that employ thousands.[30] Despite the variety of agencies, however, certain trends and traits are common across the spectrum. First, police organizations use public-conduct surveillance in several distinct ways, and the tactic is both ef-

29 *See* Jerry Ratcliffe, Intelligence-led Policing 24–25 (2008).

30 *See* Brian A. Reaves, U.S. Dep't Justice, Local Police Departments, 2007 8 (2010), *available at* http://www.bjs.gov/content/pub/pdf/lpd07.pdf.

fective for investigating crime and less expensive than conventional surveillance.[31] Second, all local-level police agencies in the United States have another common trait, cemented over decades: they receive funding for personnel, training, and equipment from the federal government.[32]

A. The Utility of GPS Surveillance for Local Law Enforcement

Technologies for public-conduct surveillance lend themselves to a range of state and local law enforcement uses, are effective at creating persuasive evidence, and are easy to employ in the field. As noted in the Introduction, public-conduct surveillance technologies range from services provided by cellular phone companies to antitheft tracking devices installed in vehicles,[33] and they can even be as simple as a transponder in a car that automatically pays tolls on the highway.[34] These technologies can be thought of as providing a spectrum of data collection capabilities, from comprehensive monitoring over long periods of time (cell phone service providers) to "snapshot" amounts of data specific to single locations at specific times (e.g., tollbooth payment information).

Thus, the most important initial observation about public-conduct surveillance technology is that it is diverse and is becoming increasingly more so, although the legal rules that govern it are not being updated accordingly. At present, the law treats surveillance relying on third-party services and tactics involving the direct acquisition of data, such as via tracking devices, very differently. The former is governed, if at all, by orders requested under the Stored Communications Act ("SCA")[35] and can be easily obtained by making a showing of relevancy to a criminal investigation;[36] the latter is regulated in an evolving, piecemeal fashion, *Jones* being the most recent example. This distinction is collapsing, however, with the proliferation of technologies which accomplish the same feat whether a third party is in-

---

31 *See infra* Part I.A.

32 *See infra* Part I.B. This trait is important for considering how a new model for regulating police surveillance might function in Part V.

33 *See supra* notes 4–6.

34 *See, e.g.*, *E-ZPass Maryland*, MD. TRANSP. AUTH., http://www.ezpassmd.com/en/home/index.shtml (last visited Mar. 31, 2012).

35 Stored Communications Act (SCA), Pub. L. No. 99-508, 100 Stat. 1860 (1986) (codified as amended at 18 U.S.C. §§ 2701–2712 (2006)).

36 *Id.*; *see In re* Application of United States for an Order Directing A Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 308–09 (3d Cir. 2010) (discussing the debate over the applicable statutory standard for historical location data and to what extent the SCA provides that standard).

volved or not, such as the use of "triggerfish" devices by law enforcement to gather cell-site location data directly without relying on an order under the SCA or any other subpoena mechanism.[37]

Public-conduct surveillance technologies may provoke some unease among privacy advocates,[38] but they are also very effective at detecting behavior indicative of criminal activity. For example, police in Fairfax, Virginia used a GPS tracking device to identify a repeat sex offender and catch him in the act of assaulting a woman,[39] and they admitted in the ensuing media coverage that they had used this warrantless surveillance approach between forty-six and sixty-one times from 2005 to 2007.[40] In the investigative context, this form of comprehensive location tracking has a natural application to conspiracy and serial offender cases, where a pattern of public movements provides powerful circumstantial evidence: the burglar is recorded, traveling from his home to his target;[41] the narcotics trafficker leads the police to his lab or his coconspirators.[42] The Virginia man caught attempting to assault a woman was partly identified using GPS records that showed his van repeatedly looping through the same neighborhoods—hunting behavior.[43] Reported cases suggest that a major use for tracking technologies has been investigating narcotics trafficking conspiracies by using the patterns of movement to identify other participants in the illicit trade.[44]

Beyond tracking a single dangerous suspect, such surveillance technology appears to lend itself to a range of state and municipal uses. Some jurisdictions have also proposed using GPS devices to

---

37 *See* William Curtiss, Note, *Triggering a Closer Review: Direct Acquisition of Cell Site Location Tracking Information and the Argument for Consistency Across Statutory Regimes*, 45 COLUM. J. L. & SOC. PROBS. 139, 162–66 (2011) (discussing the "triggerfish" technology and its ability to circumvent legal regimes governing third-party record collection).

38 *See infra* notes 136–36 and accompanying text.

39 Foltz v. Commonwealth, 698 S.E.2d 281, 283–84 (Va. Ct. App. 2010).

40 Tom Jackman, *Virginia Court: Suspect's Rights Weren't Violated by Warrantless GPS Tracking*, WASH. POST (Sept. 8, 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/09/07/AR2010090706648.html.

41 *See* People v. Weaver, 909 N.E.2d 1195, 1195–96 (N.Y. 2009).

42 United States v. Garcia, 474 F.3d 994, 995–96 (7th Cir. 2007).

43 *See* Foltz v. Commonwealth, 698 S.E.2d 281, 284 (Va. Ct. App. 2010).

44 Reported tracking device cases tend to revolve heavily around drug conspiracies. *See, e.g.*, United States v. Marquez, 605 F.3d 604, 607 (8th Cir. 2010) (marijuana trafficking); United States v. Garcia, 474 F.3d 994, 995–96 (7th Cir. 2007) (methamphetamine manufacturing); United States v. Gbemisola, 225 F.3d 753, 755–56 (D.C. Cir. 2000) (heroin shipments through the mail); United States v. Burton, 698 F. Supp. 2d 1303, 1306–07 (N.D. Fla. 2010) (cocaine trafficking).

keep track of probationers[45] and enforce court orders against stalkers and domestic abusers.[46] It has also been proposed to use the technology to create electronically monitored "liberty zones" around potential victims.[47]

One of the chief virtues of these tracking technologies for the police is that using them is quick, increasingly inexpensive, and surreptitious. A citizen is likely to only find out that he or she has been under this surveillance once it is presented as evidence in criminal proceedings. The experience of New York resident Scott Weaver is illustrative—he only found out when facing a burglary indictment that a New York State Police officer had snuck up to his van in the early morning hours and placed a tracking device beneath the bumper.[48] At trial, it was revealed that the device had monitored the vehicle's movements for sixty-five days.[49] Public-conduct surveillance technology has a natural economic advantage as well: obtaining cellular–site data records that detail one target's movements relieves the police of assigning the requisite manpower to track the suspect day-in, day-out, sometimes for weeks.[50]

Yet despite the range of uses for the technology, and its advantages over conventional visual surveillance, public-conduct surveillance technology appears to be unevenly distributed among American police departments. A study commissioned by the Justice Department and released in 2004, one of the only reports analyzing or assessing the national adoption of tracking technologies in the past decade, suggests that a pronounced urban-rural divide exists in the adoption of novel police surveillance methods.[51] The picture that emerges from the study suggests that, in the opening years of the twenty-first cen-

---

45 *See* Commonwealth v. Thissell, 928 N.E.2d 932, 933–34 (Mass. 2010).

46 *See* State v. Stevens, 646 S.E.2d 870, 871 (S.C. 2007).

47 *See* Leah Satine, *Maximal Safety, Minimal Intrusion: Monitoring Civil Protective Orders Without Implicating Privacy*, 43 HARV. C.R.-C.L. L. REV. 267, 268–69 (2008).

48 People v. Weaver, 909 N.E.2d 1195, 1195–96 (N.Y. 2009).

49 *Id.*

50 The low cost of using GPS tracking and other public surveillance methods, such as recording the location of signals to and from a cellular phone, was actually invoked by the D.C. Circuit in its *Maynard* opinion. *See infra* Part III.B.

51 *See* NAT'L INST. JUSTICE, U.S. DEP'T JUSTICE, LAW ENFORCEMENT TECHNOLOGY—ARE SMALL AND RURAL AGENCIES EQUIPPED AND TRAINED? 1 (2004), *available at* https://www.ncjrs.gov/pdffiles1/nij/204609.pdf. The study, distributed in the fall of 2000, consisted of a survey of small police agencies with fewer than 20 officers that patrolled populations of 50,000 or fewer residents, and found that GPS use among these local police departments was rare. *Id.* at 1–3, 5. Only 1.3% of these small agencies used GPS technology often for mobile surveillance, with 7.4% employing it occasionally. *Id.* Just over 90% never used it at all. *Id.* at 1–3.

tury, small police departments and their communities were not enjoying the investigative benefits of satellite tracking.[52]

Although public surveillance technologies present powerful investigative tools that could aid local police agencies with few personnel, they also present a basic temptation for the agencies with access to them. That temptation is to use these technologies to gather large amounts of information on suspected offenders for whom there is little, if any, evidence of wrongdoing before surveillance begins. This information can be said to present a "usual suspects" problem: extensive surveillance of set groups or individuals based solely on police officers' hunches, or even cultural or racial bias.

Besides the utility of these methods, another phenomenon related to these methods links the nation's law enforcement agencies. Over the last several decades, the neighborhood officer on the beat has increasingly been the beneficiary of federal funding.[53]

B. The Federal Dollar and Local Police Agencies

Although the thousands of police agencies in the United States are independently structured and pursue their own enforcement strategies, recent decades have seen substantially increased financial support from the federal government. The Omnibus Crime Control and Safe Streets Act of 1968[54] enshrined federal support for local police departments as a Congressional policy priority.[55] Among the central features of the legislation was its vision of permanent, ongoing financial support for the training, equipping, and improvement of local police agencies, starting with the funding of hundreds of millions of dollars in the programs' opening years.[56]

Subsequent decades have seen this financial relationship solidify. The Clinton Administration backed a major funding increase for local law enforcement in the mid-1990s[57] as part of the Violent Crime Control and Law Enforcement Act of 1994.[58] According to the National

---

52 *Id.*

53 *See infra* Part I.B.

54 Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197 (codified as amended in scattered sections of 18 U.S.C. and 42 U.S.C.).

55 S. REP. NO. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2117–18.

56 *Id.* at 2117–20.

57 U.S. DEP'T JUSTICE, THE CLINTON ADMINISTRATION'S LAW ENFORCEMENT STRATEGY: THE 21ST CENTURY LAW ENFORCEMENT AND PUBLIC SAFETY ACT 1 (1999), *available at* http://www.justice.gov/archive/dag/pubdoc/21st_Century.pdf.

58 Violent Crime Control and Law Enforcement Act of 1994, Pub. L. No. 103-322, 108 Stat. 1796 (codified as amended in scattered sections of 18 U.S.C. and 42 U.S.C.); *see, e.g.*, 42 U.S.C. § 13771 (2006) (authorizing grants to finance correctional facilities for violent offenders).

Institute of Justice, that legislation resulted in the hiring of 100,000 additional local police officers.[59] In 2007, when the Bush Administration found a way to cut spending by dramatically reducing the size of the law enforcement grant programs, the news drew an outcry from local police agencies that day-to-day operations would suffer.[60]

The recent financial crisis has only made local law enforcement's relationship with the federal government more explicit. The American Reinvestment and Recovery Act of 2009[61] provided more than $4 billion to state and local law enforcement, with roughly $2.7 billion distributed by the Office of Justice Programs, the traditional grant mechanism for police agencies.[62] The financial line between federal and local law enforcement has blurred.

Despite the increased sophistication of police agencies over the last two decades in terms of the use of surveillance technology and the federal government's role in financing this sophistication, federal courts still have the power to invalidate police actions through the Constitution.[63] But it is the nature of this judicial supervision, which often provides for post hoc rationalization by the police and therefore leaves space for strategic behavior, that renders its effectiveness suspect. As the next Part examines, strategic police reactions to judicial supervision are far from unusual.

II. JUDICIAL REGULATION OF POLICE AGENCIES: COMPLIANCE AND RULE NULLIFICATION

Judges regulate police agencies' behavior through constitutional rules, but compliance with those rules is far from a black-and-white choice between violation and acceptance.

The argument for expanding the Fourth Amendment's reach to encompass tracking technologies necessarily requires judges to regulate the police through the Constitution in the absence of a governing

---

59 *See Violent Crime Control and Law Enforcement Act of 1994*, NAT'L INST. JUST. (Oct. 1994), http://www.nij.gov/pubs-sum/000067.htm.

60 *See* John Gramlich, *Federal Spending Plan Slashes Anti-Crime Grants*, STATELINE (Dec. 31, 2007), http://www.stateline.org/live/details/story?contentId=267844.

61 American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115.

62 *See* OFFICE OF JUSTICE PROGRAMS, U.S. DEP'T JUSTICE, OFFICE OF JUSTICE PROGRAMS RECOVERY ACT GRANTS 1, http://www.ojp.usdoj.gov/recovery/pdfs/ojpfactsheet.pdf (last visited Mar. 31, 2012).

63 *See generally* Mapp v. Ohio, 367 U.S. 643, 655, 660 (1961) (regulating all local law enforcement by applying the Fourth Amendment's exclusionary rule against state and local agents, whereas previously the exclusionary rule had only operated in cases of federal agents violating the Constitution).

statute.[64] In deciding individual cases under the Constitution, courts often deal with specific factual scenarios involving individual officers and the suspects they arrest, not entire police departments or their programs.[65] Considering judicial supervision of the police as larger agencies, the picture that emerges suggests that, where legal ambiguities or uncertain standards control, the police respond strategically to circumvent that supervision and to further their crime control objectives. This Part concerns not how the police violate judge-imposed rules, but the strategic ways in which police *comply* with the rules—and sometimes effectively nullify the rules' purposes.

In considering institutional reactions of police agencies to judicial review of their behavior, it is useful to keep in mind that strategic reactions are likely to occur to some degree with respect to any rule adopted. Thus, strategic undercutting of a rule's purpose is best thought of as a cost that grows with the flexibility of the terms of the rule, making specific rules preferable to vague ones because they reduce the loss of rule efficacy that strategic behavior creates.[66]

The strategic behavior of police agencies takes two forms that are of particular significance for a discussion of *Maynard*. First, the police department might make slight adjustments to render their conduct constitutional while still retaining a surveillance tactic's core features. Over time, this results in a series of minor shifts as the court and the department fall into a relationship akin to that of an agency regulator and a corporation. This type of outcome has been documented and

---

64 The Fourth Amendment is a uniform regulation for all police agencies, but one whose contours are judicially imposed and developed. The principal mechanism of judicial regulation of police through the Fourth Amendment is the exclusionary rule: suppressing evidence obtained in violation of judicial interpretations of the Fourth Amendment. *See Mapp*, 367 U.S. at 648–50.

65 As applied to the police, there is typically no citizen standing to seek injunctive relief that would modify or affect an entire department's practices. *See* City of Los Angeles v. Lyons, 461 U.S. 95, 101–06 (1983) (determining that Article III standing requirements prevent a single citizen from seeking broad injunctive remedies against a police agency without a showing of ongoing or near-certain repeated personal harms). Typically in state courts, the judge is enforcing constitutional rules through a suppression hearing, which features the specific police officers who engaged in the investigative conduct and a single defendant arguing that they violated a constitutional rule. *See generally* Scott E. Sundby, Mapp v. Ohio*'s Unsung Hero: The Suppression Hearing As Morality Play*, 85 CHI.-KENT L. REV. 255, 256–64 (2010).

66 The idea of looking at police agencies as institutions with distinct interests beyond crime control is nothing new. Fourth Amendment scholar Professor Peter Swire has notably argued that police departments seek benefits and privileges from legislative bodies in much the same way that citizen groups and corporations do. *See* Peter P. Swire, Katz *Is Dead. Long Live* Katz, 102 MICH. L. REV. 904, 914–15 (2004). Professor Swire makes this observation in connection with the argument that law enforcement has an advantage in the legislative arena, making reliance on statutory limits on law enforcement surveillance powers suspect. *Id.*

can best be illustrated by judicial regulation of police checkpoints.[67] Second, police departments might formally comply with a judicial rule, but engage in other behaviors that nullify its efficacy in light of the purpose behind the rule. An example of this may be found in the interrogation context.[68]

A. Strategic Compliance: The Ballad of the Sugar Tree Road (Narcotics Interdiction Checkpoint)

The pattern of strategic police compliance has played out over the last decade in the context of narcotics checkpoints, with police making a series of minor adjustments in response to judicial rulings that left the checkpoint tactic largely unchanged in its purpose and results. The original checkpoint mechanism was straightforward: the police randomly stopped a predetermined number of vehicles to screen them with drug-sniffing dogs.[69] This system was held unconstitutional by the Supreme Court, however, on the grounds that the stops were random and not based on individualized suspicion.[70]

Police agencies in Phelps County, Missouri responded to this ruling by slightly modifying the checkpoint design for their Sugar Tree Road narcotics interdiction checkpoint in order to generate the suspicion necessary to justify the stop.[71] The new system was a ruse checkpoint.[72] Police officers set up signs along I-44 warning motorists that they were approaching a checkpoint that would feature drug dogs.[73] Drivers seeking to avoid this approaching checkpoint would take the Sugar Tree Road exit on I-44, only to discover that the real checkpoint was the exit.[74] Officers waiting on the Sugar Tree Road exit ramp were instructed to stop every vehicle that took the exit.[75] The choice of location was based on the theory that the total lack of businesses or services available there made it plain that drivers took the exit to

---

67 *See infra* Part II.A.

68 *See infra* Part II.B.

69 *See* City of Indianapolis v. Edmond, 531 U.S. 32, 35, 36 (2000).

70 *See id.* at 47–48.

71 *See* United States v. Yousif, 308 F.3d 820, 823–24 (8th Cir. 2002).

72 *See id.*

73 *See id.*

74 *See id.*

75 *See id.* at 827.

avoid police scrutiny.[76] This reason, in turn, would generate the suspicion necessary to justify the stop.[77]

This checkpoint, however, was held unconstitutional by the Eighth Circuit on much the same theory as the original design.[78] By stopping every car, the officers tacitly admitted the basis for suspicion was simply avoiding the ruse checkpoint.[79] The court held that the Constitution required more individualized suspicion for each stop.[80]

The next modification by the police was designed to create more individualized suspicion. The officers' new strategy was to premise each actual stop on minor traffic violations.[81] The officers at the Sugar Tree Road checkpoint merely observed the cars that took the exit and pulled them over for violating a particular, often minor, traffic law.[82] When the Sugar Tree narcotics interdiction effort next came under court scrutiny, the stops were no longer based purely on taking the isolated exit.[83] Instead, the drug trafficker who took the exit was pulled over for running a stop sign[84] or crossing a "fog line" with the rear wheel of a large mobile home.[85] Such a pretextual approach, premised on traffic violations despite a clear institutional emphasis on narcotics interdiction, passed constitutional muster.[86]

---

76 *See id.* at 823. This theory, that the isolation of the exit furthers an argument about suspicious behavior, has become a staple of the ruse drug checkpoint cases. *See, e.g.*, United States v. Adler, 590 F.3d 581, 582 (8th Cir. 2009) (ruse designed to convince drivers to pull off at an exit with no services or rest areas); United States v. Chavez Loya, 528 F.3d 546, 548–49 (8th Cir. 2008) (checkpoint system arranged around "dead interchange"); United States v. Martinez, 358 F.3d 1005, 1007 (8th Cir. 2004) (finding it suspicious that driver pulled off "to get something to eat" when there were no restaurants at any nearby exit).

77 *See Yousif*, 308 F.3d at 827–29.

78 *See id.*

79 *See id.*

80 *See id.* However, evasion of a checkpoint can nonetheless generate the basis for suspicion because the police can then investigate why the motorist is avoiding them. *See* United States v. Smith, 396 F.3d 579, 584–87 (4th Cir. 2005) (pulling into stranger's driveway to avoid checkpoint, followed by other suspicious behavior, created necessary suspicion for stop).

81 *See* United States v. Williams, 359 F.3d 1019, 1020–21 (8th Cir. 2004).

82 *Id.*

83 *Id.*

84 *Id.*

85 *See* United States v. Teague, 469 F.3d 205, 206–08 (1st Cir. 2006) (noting that Teague's coconspirators were caught in the Sugar Tree ruse mechanism and stopped on the theory that they had crossed the painted "fog line"). Anecdotal evidence suggests that the "fog line" violation has become a useful pretextual justification for stopping a given motorist. For an interesting empirical study of "fog line" stops in the District of Kansas, see Melanie D. Wilson, *"You Crossed the Fog Line!"—Kansas, Pretext, and the Fourth Amendment*, 58 U. KAN. L. REV. 1179 (2010).

86 *See Williams*, 359 F.3d at 1020–21.

This perfection of the "ruse checkpoint" scheme is hardly unique to Phelps County, Missouri. Federal courts have had occasion to examine similar programs in Nebraska[87] and Illinois.[88] Even under the court-approved scheme of tricking drivers into taking an isolated exit and then stopping them for a minor infraction, the police are still maintaining a fixed narcotics interdiction checkpoint that operates without any particularized evidence that a given driver is transporting narcotics. Observing the changes in checkpoint systems has led one student commentator to note that the courts appear to be imposing minor regulations on the police rather than enforcing any substantial Fourth Amendment right to privacy.[89]

The overarching imperative to interdict drugs causes the police to adhere only to the bare letter of judicial rulings and seek advantage where ambiguities exist within those rulings. The overbroad checkpoint is thus narrowed and the stops become plainly pretextual, given the fixed drug interdiction operation at the exit, but now the courts have greater difficulty in making suppression rulings.[90] Law enforcement agencies satisfy the courts' demands for some explanation by tacitly generating the suspicion necessary.

The Sugar Tree Road cases not only illustrate how the police actually modify a specific program in response to judicial interference, but also how the nature of judicial rulemaking facilitates the strategic response. The Eighth Circuit could invalidate a given practice only by ruling on each case in isolation, leaving it uncertain how the Phelps County authorities would later modify the checkpoint. Yet the Fourth Amendment is not the only body of law where this tactical shifting takes place. In the last decade, the Supreme Court has confronted

---

87 *See* United States v. Chavez Loya, 528 F.3d 546, 548–49 (8th Cir. 2008) (running a stop sign while avoiding the ruse); United States v. Gallardo, 495 F.3d 982, 984 (8th Cir. 2007) (lacking license plates while avoiding the ruse).

88 United States v. Wendt, 465 F.3d 814, 815–16 (7th Cir. 2006) (improper lane change while attempting to avoid ruse).

89 *See* Allison M. Low, Comment, *Designing a Constitutional Ruse Drug Checkpoint: What Does the Fourth Amendment Really Protect?*, 44 U.S.F. L. REV. 955, 976–77 (2010). This useful overview of checkpoint caselaw provides an excellent window into the multiple stages in checkpoint development following *City of Indianapolis v. Edmond*, 531 U.S. 32 (2000), albeit addressing it as part of a general pattern among the states. *See id.*

90 Police reliance on pretextual stops and judicial indifference to the larger motives behind a given investigative stop are anchored in the Supreme Court's ruling in *Whren v. United States*, 517 U.S. 806 (1996). *See* Timothy P. O'Neill, *Beyond Privacy, Beyond Probable Cause, Beyond the Fourth Amendment: New Strategies for Fighting Pretext Arrests*, 69 U. COLO. L. REV. 693, 693–94 (1998) (discussing *Whren's* de facto endorsement of police tactics that rely on minor infractions to investigate crimes for which no probable cause or other evidence existed prior to the stop and search).

strategic behavior that led to the outright nullification of a judicial rule in the context of interrogations.

B. Compliance Leads to Rule Nullification: Interrogations

Law enforcement's strategic compliance with and nullification of judicial rules is made even more explicit in the context of interrogations. Under *Miranda v. Arizona*,[91] statements taken from a criminal suspect in custody prior to being apprised of his or her procedural rights are inadmissible at trial.[92] Such an approach left open the possibility that pre-*Miranda*-warning conduct by the police could nullify the *Miranda* warning's effect. The Court took up that issue in *Oregon v Elstad,*[93] approximately nineteen years after *Miranda* was decided.[94]

Prior to being given his Miranda warnings, Michael Elstad made a statement implicating himself in a burglary while under arrest at his mother's home.[95] He was advised later of his rights at the police station and then made a series of incriminating statements.[96] On appeal, Elstad contended that the postwarning statements should be suppressed because his initial, prewarning statement "let the cat out of the bag," resulting in a form of compulsion.[97] The Supreme Court rejected that argument, concluding that prewarning questioning did not affect the admissibility of postwarning statements.[98]

The reaction of law enforcement agencies with respect to that rule became clear in 2004, when the Court considered *Missouri v. Seibert*.[99] Patrice Seibert was suspected of involvement in the mobile home arson that left her disabled son and another youth dead.[100] She was thoroughly interrogated at the police station, and only after admitting her culpability were *Miranda* warnings given to her.[101] Then, her interrogators walked her through the prewarning admissions, one

---

91 Miranda v. Arizona, 384 U.S. 436 (1966).

92 *See id.* at 492–93.

93 Oregon v. Elstad, 470 U.S. 298 (1985).

94 *See id.*

95 *See id.* at 300–01.

96 *See id.* at 301.

97 *Id.* at 302.

98 *Id.* at 317–18.

99 Missouri v. Seibert, 542 U.S. 600 (2004) (plurality opinion); *see also* Christian Halliburton, *Leveling the Playing Field: A New Theory of Exclusion for a Post-PATRIOT Act America*, 70 MO. L. REV. 519, 532–34 (2005) (discussing *Seibert* as a strategic effort to undermine judicial supervision of police behavior in the interrogations context).

100 *Seibert*, 542 U.S. at 604–05.

101 *Id.* at 604–06.

at a time.[102] This case was hardly a lone instance of creative policing; the tactic was outlined in the department's training manual.[103] The Missouri police officers admitted that they were consciously avoiding the strictures of *Miranda*,[104] and the state government argued on appeal that the police were entitled to do so under *Elstad*.[105]

What is striking about *Seibert* is that it constitutes a particularly straightforward case of law enforcement agencies pursuing their interests in crime control. *Miranda* imposed a cost on the police: the increased likelihood that a warned suspect will avoid making self-incriminating remarks. *Elstad* created a potential for prewarning interrogation that would have no effect on the admissibility of postwarning statements.[106] *Seibert* is the natural institutional reaction: the two-step confession formally complies with the judicial rule and is codified as a method that essentially nullifies *Miranda's* intended effect.

The above examples suggest that strategic agency behavior in response to judicial rulemaking becomes more likely to arise when rules are uncertain and highly fact-specific. *Edmond* invalidated checkpoint seizures conducted without suspicion, so the Phelps County police kept modifying the design until federal courts found some minimal level of suspicion to justify a functionally similar practice.[107] *Miranda* imposed a procedural constraint on interrogations, but *Elstad* permitted some prewarning questioning, so interrogators developed the two-step technique to render the warnings meaningless.[108] An insufficiently specific judicial rule on the use of long-term monitoring under the Fourth Amendment would likely be subject to this same process; the greater the uncertainty in the monitoring standard, the greater the costs imposed through strategic behavior.

III. THE DEFECTS OF A REGULATORY MODEL ORGANIZED AROUND PRIVACY RIGHTS: THE *KATZ V. UNITED STATES* PRECEDENT AND *UNITED STATES V. MAYNARD*

The expansive privacy theory advanced by the D.C. Circuit's opinion in *United States v. Maynard* creates opportunities for strategic behavior in relation to the threshold question of whether the Fourth

---

102 *Id.* at 605–06.

103 *Id.* at 609–10.

104 *Id.* at 605–06.

105 *Id.* at 614–15.

106 *See supra* text accompanying notes 95–98.

107 *See supra* Part II.A.

108 *See supra* Part II.B.

Amendment even applies to a given surveillance tactic.[109] This problematic approach persists as an answer to the unresolved question of *Jones*: the evaluation of monitoring without physical trespass.[110] *Maynard's* vision of privacy interests reflects recent demands by scholars for a Fourth Amendment standard that addresses and protects public conduct from surveillance.[111] In that sense, the opinion's defects are the defects of a school of thought that relies upon privacy protection as the means of regulating the police. *Maynard* is the high watermark of a theory of privacy that introduces procedural defects through creating damaging uncertainty.[112]

The question of whether a given police tactic is regulated by the Fourth Amendment depends upon a finding that the tactic constitutes a search or seizure[113]—a threshold inquiry that *United States v. Maynard* addressed by holding that GPS tracking, with or without device attachment, is a search.[114] The Supreme Court has developed a test for assessing when nontrespassory official conduct constitutes a search, first articulated by Justice Harlan in *Katz v. United States*[115] in 1967. The test consists of two inquiries: first, whether the individual has demonstrated an expectation of privacy through his or her actions, and second, whether that is a privacy claim that society accepts as reasonable.[116]

Katz entrenched privacy in Fourth Amendment surveillance law.[117] In the context of tracking public movements using novel technologies, the *Katz* test was applied in *United States v. Knotts*.[118] The *Katz-Knotts* precedent forms the foundation upon which the constitutional arguments about nontrespassory monitoring must rest. Ultimately, *Maynard's* expansion of those arguments suggests that a focus

---

109 This problem is discussed more fully in Part III.C.

110 *See infra* Part IV.

111 *See infra* text accompanying notes 136–37.

112 That particular defect in *Maynard's* standard is explored below. *See infra* Part III.C.

113 The Fourth Amendment provides a right to be free of unreasonable "searches and seizures." U.S. CONST. amend. IV.

114 *See infra* Part III.B.

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

116 *Id.*

117 *See* Swire, *supra* note 66, at 904 ("*Katz v. United States* is the king of Supreme Court surveillance cases. Written in 1967, it struck down the earlier regime of property rules, declaring that 'the Fourth Amendment protects people, not places.' The concurrence by Justice Harlan announced the new regime—court-issued warrants are required where there is an infringement on a person's 'reasonable expectation of privacy.'" (footnotes omitted)).

118 United States v. Knotts, 460 U.S. 276, 280–81 (1983).

on privacy in this area limits the effectiveness of the resulting rules because it creates opportunities for strategic police behavior.

A. United States v. Knotts *and Its Progeny*

The Supreme Court laid a foundation for Fourth Amendment claims regarding the tracking of public conduct in its 1983 opinion, *United States v. Knotts*. In *Knotts*, government agents placed a tracking device that emitted radio signals, known as a "beeper," in a drum filled with a chemical used in the manufacture of methamphetamine.[119] Agents simply tracked the drum to an isolated cabin by following the signals.[120] The tracking device served as a supplement to, and eventually a replacement for, visual surveillance by government agents: at one point, they lost sight of the vehicle transporting the drum and had to rely on the signal to find its location.[121]

Knotts contended that the use of the tracking device to follow his coconspirator's route and discover the location of his coconspirator and Knotts' cabin was a Fourth Amendment search.[122] The Court rejected his argument as falling outside the *Katz* precedent for defining Fourth Amendment searches based on privacy interests.[123] Performing the two-pronged *Katz* analysis, the Court first observed that "[a] car has little capacity for escaping public scrutiny,"[124] and then it evaluated the second prong—whether there was an objective, reasonable privacy interest in the vehicle's movements as revealed by the beeper.[125] The Court heavily based this second-prong analysis on the observation that conventional surveillance by police officers on the road would reveal the same data.[126] After noting this, the Court dismissed an expectation of privacy in public movements along a journey as unreasonable.[127] The Fourth Amendment did not apply to surveillance using beeper technology on public roads.[128]

---

119 *Id.* at 278–79.

120 *Id.*

121 *Id.*

122 *Id.* at 279.

123 *Id.* at 281–82.

124 *Id.* at 281 (quoting Cardwell v. Lewis, 417 U.S. 583, 590 (1974) (plurality opinion)).

125 *Id.* at 281–82.

126 *Id.* at 281–84.

127 *Id.* at 283–85.

128 *Id.* Unsurprisingly, the academic reaction to the opinion was cast in terms of the potential violations of privacy rights rendered legitimate by the holding. *See* Note, *Tying Privacy in* Knotts*: Beeper Monitoring and Collective Fourth Amendment Rights*, 71 VA. L. REV. 297, 321–26 (1985).

The *Knotts* principle was left undisturbed by the *Jones* decision. By relying on a trespassory theory of searches, rather than addressing the lack of a privacy interest in public conduct, Justice Scalia's majority opinion expressly avoids undercutting the *Knotts* proposition about nontresspassory monitoring.[129] Although Justice Sotomayor's and Justice Alito's concurrences each raised the problem of nontrespassory monitoring,[130] the Court has nonetheless left the *Knotts* principle intact.

Between 2006 and the decision in *Maynard*, which the Supreme Court affirmed, the Seventh, Eighth, and Ninth Circuits addressed the *Knotts* precedent and held that monitoring did not present a constitutionally novel issue.[131] In the 2010 case *United States v. Pineda-Moreno*,[132] the Ninth Circuit rejected the argument that the more comprehensive record generated by modern tracking technologies was of constitutional import and quoted *Knotts*: "We have never equated police efficiency with unconstitutionality and decline to do so now."[133] These cases describe *Knotts* as a controlling precedent that does not provide for Fourth Amendment regulation when all that has been tracked is movement on a public thoroughfare—a narrow conception of privacy that excludes public behavior.

Academic commentary during the past decade (when these cases were decided) has defined these issues in terms of personal privacy, but has diverged from the logic of the recent opinions under *Knotts* in that it favors a broader definition of what is private. At present, police surveillance is a legal issue analyzed through the lens of privacy rights by professorial[134] and student commentators,[135] with the result that privacy theories must continually expand to encompass each new surveillance technology. Professor Renee Hutchins, writing in 2007, argued that location tracking is a search if it reveals such a large vol-

---

129 *See* United States v. Jones, 132 S. Ct. 945, 951–53 (2012) (distinguishing *Knotts* on the lack of trespassory search in that case).

130 *See id.* at 954–55 (Sotomayor, J., concurring in the judgment); *id.* at 957–59 (Alito, J., concurring in the judgment).

131 *See* United States v Pineda-Moreno, 591 F.3d 1212, 1215–17 (9th Cir. 2010), *vacated*, No. 10-7515 (U.S. Feb. 21, 2012); United States v. Marquez, 605 F.3d 604, 609 (8th Cir. 2010) (finding in the alternative that, even if the defendant-appellant had standing, *Knotts* rendered his Fourth Amendment claim invalid); United States v. Garcia, 474 F.3d 994, 997–99 (7th Cir. 2007).

132 United States v. Pineda-Moreno, 591 F.3d 1212 (9th Cir. 2010), *vacated*, No. 10-7515 (U.S. Feb. 21, 2012).

133 *Id.* at 1216 (quoting Knotts v. United States, 460 U.S. 276, 284 (1983)).

134 *See infra* notes 136–36 and accompanying text.

135 *See* Plourde-Cole, *supra* note 7, at 613–14 (arguing that such tactics should be governed by a warrant requirement because they implicate a privacy interest).

ume of otherwise public information about a given person that her privacy is violated.[136] She concluded that shared social expectations that one citizen will not be comprehensively tracked thus render that privacy interest objectively reasonable under *Katz* and *Knotts*.[137] Professor Hutchins's thesis is an extension of arguments for expanding privacy rights from the past decade. Professor Christopher Slobogin's observation in 2002 that citizens have a right to a kind of public privacy—the right to travel and act unrecorded[138]—or Professor Dorothy Glancy's 2004 discussion of legal recognition of "privacy on the open road,"[139] are just two relevant examples of those discussions.

The D.C. Circuit adopted this school of thought in *United States v. Maynard*, and the Supreme Court majority neither endorsed nor rejected it in reaching its decision in *Jones*.[140] The *Maynard* opinion is the first by a federal appellate court that argues for expanding the Fourth Amendment's regulatory reach by expanding the definition of privacy beyond the plain language of *Knotts*.[141] In that sense, *Maynard's* failings are the failings of an expansive, privacy-centered approach to regulating public-conduct surveillance technologies.

B. United States v. Maynard

On August 6, 2010, the D.C. Circuit became the first federal appellate court (since *Knotts* was decided) to hold that the Fourth Amendment regulates comprehensive tracking of a citizen's public movements.[142] In doing so, the Court relied upon two distinct privacy theories: first, that privacy rights are violated through extensive compilation of public data, and second, that the presumption of an individual expectation of privacy in public conduct need not be shown by specific individual acts.[143] This approach accords with demands by scholars for a broader vision of privacy under *Katz*, but its uncertain boundaries ultimately reveal that privacy is a poor theory to explain the regulation of public-conduct surveillance.

---

136 Hutchins, *supra* note 9, at 459–60.

137 *Id.* at 458.

138 Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 Miss. L.J. 213, 217–18 (2002).

139 *See* Dorothy J. Glancy, *Privacy on the Open Road*, 30 Ohio N.U. L. Rev. 295, 295–96 (2004).

140 United States v. Jones, 132 S. Ct. 945 (2012).

141 *See* United States v. Maynard, 615 F.3d 544, 561–65 (D.C. Cir. 2010), *aff'd on other grounds sub nom. Jones*, 132 S. Ct. 945; *see also supra* notes 131–32 and accompanying text.

142 *Maynard*, 615 F.3d at 561–65.

143 *Id.*

In *Maynard*, Antoine Jones and Lawrence Maynard were indicted on federal drug trafficking charges and ultimately convicted at trial.[144] Jones's participation in the conspiracy was demonstrated through GPS evidence, in addition to property and cellular phone records.[145] He moved to suppress the GPS records of his public movements, but the district court, relying on *Knotts*, denied the motion insofar as it related to public travels on the road.[146] The prosecution had repeatedly referred to and relied upon detailed records of Jones's driving patterns, obtained through the placement of a tracking device on a Jeep he regularly drove, which monitored his position continuously for twenty-eight days.[147] On appeal, the D.C. Circuit reversed Jones's conviction and held that the collection of data from the GPS device was a Fourth Amendment search that required a warrant to be constitutional.[148] As a result, the evidence obtained should never have been admitted at trial pursuant to the exclusionary rule.[149]

Essential to the court's holding was its recognition of an objectively reasonable, socially accepted privacy interest in the totality of one person's public movements.[150] Writing for the panel, then-Judge Ginsburg explained: "A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband . . . and not just one such fact about a person, but all such facts."[151] Arguing that no individual actually displays all of his or her public movements to anyone and that constant visual surveillance is so prohibitively expensive as to be unlikely to occur, the court found an objective privacy interest affected by the aggregation of GPS data over time.[152]

In its analysis, the court seized upon a basic ambiguity in the *Katz* test: whether an expectation of privacy is reasonable because the subject matter is typically not scrutinized in practice, which is an empirical question about probability, or because it is not legally or

144 *Id.* at 544.

145 *Id.* at 567–68.

146 United States v. Jones, 451 F. Supp. 2d 71, 87–88 (D.D.C. 2006), *rev'd sub nom. Maynard*, 615 F.3d 544, *aff'd on other grounds sub nom. Jones*, 132 S. Ct. 945. The district court did allow for suppression of data recovered from the vehicle when it was parked in Jones's attached garage, on the theory that such information was private under existing precedent. *Id.*

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

148 *Id.* at 566–68.

149 *Id.*

150 *See id.* at 563.

151 *Id.* at 562.

152 *Id.* at 563–66.

customarily permitted, which is a normative question.[153] The *Maynard* court found an objectively valid privacy interest on the basis of the former, and not the latter.[154]

To distinguish *Knotts*, the D.C. Circuit notably cited Professor Renee Hutchins's 2007 article advancing the probability argument, further underscoring that the past decade's scholarly commentary influenced the opinion.[155] In a footnote, for a proposition seemingly unrelated to the thrust of the court's argument, Hutchins's 2007 article appears.[156] This is an unlikely coincidence: Hutchins argued in that article that the volume of information collected by weeks of tracking violates a shared social expectation that so much data would never be collected,[157] and this is the centerpiece of the *Maynard* opinion.[158] Further illustrating the opinion's scholarly underpinnings is that it relied on privacy tort cases and state legislation,[159] both approaches that commentators had identified as legal support for this privacy interest.[160].

This conception of privacy adopted in the opinion has been termed the "mosaic theory"—the idea that "the whole is greater than the sum of its parts."[161] At some point after tracking Jones for a single trip, which does not constitute a search under *Knotts*, but before the tracking had been going on for four weeks, it became a search within the meaning of the Fourth Amendment.[162] Aggregating data creates the mosaic—and thus triggers the constitutional protection of privacy, because the public at large would not expect such comprehensive monitoring.

---

153 *See* Florida v. Riley, 488 U.S. 445, 453–55 (1989) (O'Connor, J., concurring) (arguing that what determines an expectation's legitimacy is a social understanding about what is commonly done, not what is legally possible, and questioning the plurality opinion's reliance on FAA regulations to demonstrate officers' lawful vantage point).

154 *Maynard*, 615 F.3d at 559 ("[W]e ask not what another person can physically and may lawfully do but rather what a reasonable person expects another might actually do.")

155 *Id.* at 565 n.*.

156 *Id.* The footnote cites Hutchins's article solely for the point that tracking devices can now be attached via dart, and then immediately cites a news story to convey the same point. *Id.* The citation to Hutchins is superfluous, except that the court is signaling the adoption of that article's argument.

157 *See* Hutchins, *supra* note 9, at 455–59.

158 *Maynard*, 615 F.3d at 563–66.

159 *Id.* at 564.

160 *See, e.g.*, Glancy, *supra* note 139, at 352–55.

161 *Maynard*, 615 F.3d at 560–66; *see also* Bethany L. Dickman, Note, *Untying* Knotts*: The Application of Mosaic Theory to GPS Surveillance in* United States v. Maynard, 60 AM. U. L. REV. 731, 737–42 (2011).

162 *Maynard*, 615 F.3d at 563–66.

Even assuming that aggregating data about an individual violates a privacy interest that society recognizes, the opinion expanded past privacy doctrine in another way that contributes to its standard's uncertainty. The *Maynard* court's analysis presumed that an individual demonstrates an expectation of privacy when he or she travels on public roads.[163] In other words, it dispenses with the first prong of the *Katz* analysis entirely: no specific conduct need be shown that reflects a desire for privacy.[164]

As the Supreme Court held in *Smith v. Maryland*,[165] a case that the D.C. Circuit cited in its *Maynard* opinion,[166] the determination that a given police tactic is a search requires first that individuals demonstrate through their conduct a subjective expectation of privacy.[167] Only then does the analysis proceed to acceptance of that expectation as reasonable.[168] What unites the cases that construed *Katz* over the last four decades is that their analysis requires the citizen to point to some choice or action that suggests a desire to keep something private.[169] But a driver on a public highway cannot demonstrate a subjective expectation of privacy specific to his or her movements, because there is no way to conceal the trip. There is no practical way to distinguish a driver going about a daily routine from a driver who subjectively expects no one to discover that routine. That is the fundamental difference between driving and activities like placing personal items in an opaque piece of luggage[170] or covering marijuana plants with a greenhouse[171]—activities that the Supreme Court

163 *See id.* at 559–63.

164 The Supreme Court often grants the point in its opinions and defeats the claimed expectation of privacy on *Katz's* second, objective prong—but that is not the same thing as dispensing with the analysis entirely. *See* Renée McDonald Hutchins, *The Anatomy of a Search: Intrusiveness and the Fourth Amendment*, 44 U. RICH. L. REV. 1185, 1192–94 (2010) ("[T]he second prong of the *Katz* analysis—objective reasonableness—has come to do much of the heavy lifting.").

165 Smith v. Maryland, 442 U.S. 735 (1979).

166 *Maynard*, 615 F.3d at 561 (citing *Smith*, 442 U.S. at 742–43).

167 *See Smith*, 442 U.S. at 740.

168 *Id.* at 742–44.

169 Perhaps the only consistent exception to the affirmative conduct requirement is when the government seeks to obtain and analyze bodily material, such as DNA or urine. *See, e.g.*, Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 617–19 (1989) (considering urinalysis a search but making no mention of *Katz*). Of course, it is unclear how one could demonstrate through conduct a privacy interest in the substance of one's physical self.

170 Bond v. United States, 529 U.S. 334, 338 (2000).

171 Florida v. Riley, 488 U.S. 445, 450–51 (1989) (plurality opinion) (finding Riley's expectation of privacy unreasonable because aerial overflights by helicopter or plane are common in society).

has considered manifestations of at least a subjective expectation of privacy.

The omission of the first prong from the opinion is significant because it converts privacy into a kind of protected space around each individual, irrespective of the citizen's specific conduct.[172] The *Jones* majority avoided this issue by confining its analysis to physical interaction with property, rather than examining the continued viability of the two-prong *Katz* analysis.[173] The *Maynard* approach reconfigures *Katz* as being solely about social expectations of privacy.[174]

Maynard does not just trivialize the affirmative conduct requirement, however—the opinion's standard abandons it. *Maynard* rewrites *Katz* by dismantling its first prong and treating public movements as inherently private, at least in the aggregate.

In this sense, *Maynard* creates an approach to the Fourth Amendment where the individual has an automatic privacy interest in public behavior, a privacy interest that is violated at some undefined point as the police track that individual for days. The *Maynard* court's holding is not necessarily incorrect in its recognition of this privacy interest, nor are the many scholars who make similar arguments, but the opinion's departure from precedent is a conceptual problem as well as a legal one. A body of constitutional rules for public surveillance technologies, built on a theory about privacy that neither requires specific conduct by an individual nor identifies exactly when privacy has been violated, makes determining what is "private"—and therefore the proper subject of constitutional protection—all but impossible.[175]

Beneath its conflict with the privacy-centered *Katz* precedent, *Maynard* also illustrates a subtle problem. Its flexible standard for when the Fourth Amendment is triggered creates the opportunity for

---

172 This conception ultimately aligns with Professor Christopher Slobogin's vision of public privacy, although he bases his conclusion on the combination of distinct strands of existing law rather than the notion that a person has a continuous, automatic privacy interest, even if the net effect for doctrinal purposes is the same. *See* Slobogin, *supra* note 138, at 217–18.

173 *See* United States v. Jones, 132 S. Ct. 945, 953–54 (2012).

174 *See* United States v. Maynard, 615 F.3d 544, 558–60 (D.C. Cir. 2010), *aff'd on other grounds sub nom. Jones*, 132 S. Ct. 945. The court refers to multiple cases that provided explicit reference to the two-pronged nature of *Katz* analysis, but never quotes that language or paraphrases that aspect of the precedent. *Id.*

175 Professor Orin Kerr has argued in past articles that the privacy protection afforded by the *Katz* framework tends to shift depending on how familiar a reviewing court is with the surveillance tactic at issue. *See, e.g.*, Kerr, *supra* note 11, at 806–07. Where property interests are clearly at stake, privacy protection is more easily delineated; but where they are not, the lines begin to blur. *See id.*

strategic police behavior along the lines discussed in Part II, which the following Section explores.

C. Maynard*'s Hidden Flaw: How Privacy Theories Could Facilitate Strategic Behavior*

The D.C. Circuit in *Maynard* was able to find that a search took place only by creating the most expansive theory of Fourth Amendment privacy yet put forth by a federal appellate court. The *Maynard* theory has since prompted both praise and criticism for its vigorous defense of privacy rights or its unworkable attempt to do so.[176] That theory, however described, survives the *Jones* decision because it is focused on monitoring and not trespass, as recognized by a decision from the District of Maryland in March 2012.[177] But this standard for evaluating public-conduct monitoring, because of the uncertainty inherent in it, is rife with the potential for the types of strategic police behavior discussed in Part II. This Section examines the uncertainty of the *Maynard* standard in greater detail and uses a recent application of that standard where no physical trespass took place to illustrate the opportunities for strategic police behavior that it produces.[178]

The D.C. Circuit in *Maynard* created a significant doctrinal gap between its new "mosaic theory" standard and the *Knotts* precedent. The court held that, under *Knotts*, no search occurred when the police tracked a motorist along a single journey, but that the precedent did not apply when the police engaged in prolonged recording.[179] In *Maynard*, Jones's public movements behind the wheel of his Jeep were tracked over a period of twenty-eight days;[180] in *Knotts*, when Knotts's coconspirator was being tracked, it was a single trip to an isolated

---

176 *Compare* Benjamin M. Ostrander, Note, *The "Mosaic Theory" and Fourth Amendment Law*, 86 NOTRE DAME L. REV. 1733 (2011) (arguing that *Maynard* is impractical as a defense of privacy rights and that Congress should provide the necessary privacy protections through statute), *with* Erin Smith Dennis, Note, *A Mosaic Shield:* Maynard*, the Fourth Amendment, and Privacy Rights in the Digital Age*, 33 CARDOZO L. REV. 737 (2011) (arguing that *Maynard* is an important new doctrinal development in constitutional privacy theory)

177 *See* United States v. Graham, No. RDB-11-0094, 2012 WL 691531, at *10 (D. Md. Mar. 1, 2012). Although Justice Alito's concurrence in *Jones* concluded, in line with *Maynard*, that when it comes to the infringement of privacy rights through remote monitoring, after four weeks "the line was surely crossed," United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring), the majority opinion relied strictly on property-based reasoning and offered no opinion on the *Maynard* standard in affirming the panel's decision, *id.* at 949–54 (majority opinion).

178 *See infra* text accompanying notes 226–29.

179 United States v. Maynard, 615 F.3d 544, 566–68 (D.C. Cir. 2010), *aff'd on other grounds sub nom. Jones*, 132 S. Ct. 945.

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

cabin.[181] The *Maynard* court held that while a motorist like Knotts may have no objectively reasonable expectation of privacy in a single trip because other citizens along the route would observe the journey, weeks of driving would not actually be observed by another individual.[182] Prolonged surveillance, aggregating a large amount of data on public movements, thus violated Jones's right to privacy. In sum, the *Maynard* court concluded that at some point between a single trip and weeks of surveillance, the privacy interest is violated and the Fourth Amendment kicks in.[183]

But such an approach leaves it entirely unclear how prolonged the tracking must be to trigger the Fourth Amendment's protections, creating a gap between applicable rules. If *Knotts* only provides that no search takes place when a tracking device is used over a brief span of time and *Maynard* holds that the same police tactic becomes a search when conducted over the course of four weeks, there is no natural privacy-based point at which to make the distinction. Should the Fourth Amendment kick in after more than one trip is being recorded? After a week?

A February 2011 district court opinion demonstrates the uncertainty of the *Maynard* standard and suggests that it creates opportunities for strategic behavior. Magistrate Judge James Orenstein of the Eastern District of New York reviewed a federal government application to retrieve location data for a particular suspect from a cell phone service provider.[184] Because obtaining those records would reveal patterns of a citizen's public movements, much like the use of a GPS device, Judge Orenstein invoked the *Maynard* approach to determine whether the Fourth Amendment was implicated by the request.[185] *Maynard's* theory, however, proved to be a poor guide. In this instance, the government did not seek a solid month's worth of public location data; it sought only a set of distinct periods, totaling twenty-one days.[186] The breaking up of the total surveillance into periods of three days, six days, and twelve days led Judge Orenstein to conclude that the data being collected was insufficiently comprehensive to trig-

---

181 United States v. Knotts, 460 U.S. 276, 278–79, 285 (1983).

182 *Maynard*, 615 F.3d at 558–60.

183 The D.C. Circuit avoided this issue by only addressing the surveillance conducted with respect to Jones. *Id.* at 555–66.

184 *In re* Application of United States for an Order Authorizing the Release of Historical Cell-Site Information, No. 11-MC-0113(JO), 2011 WL 679925, at *2 (E.D.N.Y. Feb. 16, 2011).

185 *Id.*

186 *Id.*

ger the *Maynard* privacy standard.[187] Note the net effect: the government still obtains nearly the same amount of public conduct information—twenty-one days of movements instead of the twenty-eight days in *Maynard*—but the Fourth Amendment is not triggered because the monitoring is in discrete blocks rather than a continuous period.[188] Although Judge Orenstein may have set a distinct outer limit for when monitoring becomes a search, there is no indication why twenty days of tracking does not violate a privacy interest, but thirty days does.[189] Whatever might explain such a distinction, a privacy theory does not.[190]

The difficulties of applying *Maynard* for assessing when the Fourth Amendment is implicated will encourage precisely the sort of strategic police reactions discussed above.[191] One can imagine a series of opinions, along the lines of Judge Orenstein's analysis, attempting to parse out when the surveillance tactic revealed so much public information that it became a search. Each opinion would, in turn, trigger a strategic response—slight deviations in the extent of the recording, perhaps, or discrete blocks of surveillance rather than continuous recording.[192] Whereas the examples discussed in Part II—checkpoint stops and interrogations—both featured some amount of strategic behavior in response to the application of established consti-

187 *See id.* ("I do not mean to suggest that I can or should define the minimum duration that transforms the kind of discrete surveillance effort at issue in *Knotts* into the sustained location tracking that triggers the warrant requirement under *Maynard*. I venture no further than the appellate court that decided *Maynard*.")

188 *See id.*

189 *See id.*

190 Reflecting the uncertainty of this privacy theory is the fact that the reaction to *Maynard* among the federal courts has been mixed, with the Fifth Circuit construing the opinion narrowly, *see* United States v. Hernandez, 647 F.3d 216, 220–21 (5th Cir. 2011) (distinguishing *Maynard* based on length of tracking), and the Western District of Michigan, the District of South Carolina, and the District of Maryland rejecting the theory outright, *see* United States v. Graham, No. RDB-11-0094, 2012 WL 691531, at *16–17 (D. Md. Mar. 1, 2012); United States v. Narrl, 789 F. Supp. 2d 645, 651–52 (D.S.C. 2011); United States v. Walker, 771 F. Supp. 2d 803, 807, 809–12 (W.D. Mich. 2011). By contrast, in addition to Judge Orenstein's endorsement, the Southern District of Texas embraced the *Maynard* rationale in October of 2010 in the context of cell-site location data requests under the SCA. *See In re* Application of the United States for Historical Cell Site Data, 747 F. Supp. 2d 827, 838–40 (S.D. Tex. 2010) (invoking *Maynard*'s analysis to apply the Fourth Amendment to requests for cell-site data from third-party service providers).

191 *See supra* Part II.

192 Judge Orenstein's analysis would certainly suggest that breaking up the monitoring period would give the government a plausible argument for why *Maynard* did not address the facts of the case. *See supra* text accompanying notes 184–86. This of course would facilitate a distinct form of post hoc rationalization—a continuous strategy of testing how many discrete blocks of surveillance would be required to evade the warrant requirement.

tutional rules to their prior behavior,[193] the *Maynard* analysis allows for strategic behavior on the question of whether the Fourth Amendment even applies to the tactic at issue.

This is not to cynically claim that every police department would automatically react to and attempt to evade *Maynard's* standard; it is only an observation that sufficient circumstantial evidence already exists to show that such a response by some departments is likely. The same pressure to produce results and combat crime would exist in an investigation employing public-conduct surveillance as it does in highway drug interdiction efforts or investigations relying on successful interrogations of suspects.[194] *Maynard's* unclear standard invites further judicial rulemaking, but Judge Orenstein's opinion underscores how especially difficult it is for a court embracing *Maynard's* privacy theory to establish limits when that privacy theory is untethered to property or any other natural dividing line. As has been demonstrated in other contexts, the greater the uncertainty in a standard, the more it facilitates evasion, which in turn reduces the efficacy of judicial power as a check on arbitrary police conduct.[195]

If the uncertain judicially created standard of *Maynard* invites strategic responses to case-by-case evaluation of surveillance programs, the proposed GPS Act could provide much-needed clarity through legislative action. Unfortunately, the statute as proposed falls short of the task, as the next Part demonstrates.

IV. THE GPS ACT: CONGRESS GOES TOO FAR . . . AND NOT FAR ENOUGH

If the *Maynard* approach to regulation, bringing public-conduct surveillance technologies under the Fourth Amendment's reach through an uncertain privacy theory, is unworkable because it allows for too much strategic undercutting by the police, then Senator Wyden's proposed GPS Act suffers from the defect of too broadly limiting socially beneficial law enforcement conduct in a manner that makes little sense in light of existing law or a theory of citizen privacy.

Although the best should not be made the enemy of the good, the current proposed legislation perpetuates the long-standing congressional approach to regulating surveillance technologies, resulting in

---

193 Those examples each describe areas of criminal procedure where the police are not required by the courts to obtain any external permission or have an official record prior to stopping or interrogating a citizen. *See supra* Part II.

194 *See supra* Part II.

195 *See infra* Part V.

doctrinal inconsistency and applying a counterproductive one-size-fits-all approach to every surveillance tactic that tracks a target's public movements. This has the added policy defect of continuing to leave amendment and new regulation to express legislation by Congress—a body that often takes decades to address new surveillance technologies. To understand why the Act's specific provisions are an unsatisfactory alternative to the *Maynard* approach, Congress's prior technology-based surveillance legislation must be briefly examined.

A. The Legislative Approach to Surveillance Technologies Prior to 2010

Congress's two major forays into regulating new surveillance technologies with legislation—statutes covering wiretapping[196] and the use of pen registers (which record the origin and destination of communications like phone calls, but not their contents)[197]—have each been dependent on the constitutional decisions of the Supreme Court. Decades, moreover, elapsed between these legislative interventions and constitutional decisions in the surveillance technology arena.

From a privacy standpoint, Congress's commitment to imposing meaningful constraints on the police is currently based on the minimum standards established by the Supreme Court. Although the use of both wiretaps and pen registers are tactics regulated by federal law, their treatment under the Constitution could not be more different. In *Katz v. United States*, the Supreme Court held that recording a private phone call among two unaware individuals was a Fourth Amendment search and therefore required a probable cause-based warrant.[198] This ruling spurred Congress to create a statutory framework for the practice.[199] By contrast, in *Smith v. Maryland*, the Court found that no search occurred when pen registers were used, leaving unaddressed how such tactics should be regulated.[200] Because of the difference in constitutional treatment, the standards Congress created for obtaining a court order differ significantly. Wiretapping was first brought under comprehensive federal statutory control in Title III of the Omnibus Crime Control and Safe Streets Act of 1968,[201] and pen

196 *See, e.g.*, 18 U.S.C. § 2510 (2006) (defining the regulated wiretapping practice as interception of electronic or oral communications).

197 *See* Smith v. Maryland, 442 U.S. 735, 741–42 (1979).

198 *See* Katz v. United States, 389 U.S. 347 (1967)

199 *See* S. REP. 90-1097, 1968 U.S.C.C.A.N. 2112.

200 *See Smith*, 442 U.S. at 736, 746.

201 Omnibus Crime Control and Safe Streets Act of 1968, Pub. L 90-351, 82 Stat. 197 (codified as amended in scattered sections of 18 U.S.C. and 42 U.S.C.).

registers were brought under congressional regulation with the adoption of the Electronic Communications Privacy Act of 1986.[202] Title III imposes a full probable-cause warrant requirement,[203] while the pen register statutory provisions allow for an order authorizing surveillance to be issued on a showing of mere relevancy to a criminal investigation.[204]

This approach in these areas—taking action on a particular technology in isolation with express legislation—has the additional effect of making congressional action on surveillance law relatively rare. Note that nearly two decades elapsed between the enactment of laws governing recording verbal conversations and laws governing the aggregation of telephone numbers, and more than two decades elapsed before Senator Wyden proposed a bill to do the same for monitoring public movements. The GPS Act thus presents a continuation of a pattern of slow legislative responses to emerging technologies, and as the next Section explores, its substantive provisions raise policy problems as well.

B. The GPS Act and Its Shortcomings

The GPS Act's substantive provisions have a principal defect: the proposed statute applies a broad probable cause requirement to virtually any request from a service that collects location data. The Act goes too far in its demands on the police through this across-the-board probable cause warrant requirement. The proposed statute governs all "geolocation information," which is defined as "any information . . . concerning the location of a wireless communication device . . . that could be used to determine or infer information regarding the location of the person."[205] The ability to obtain this information is dependent on the issuance of a warrant based on probable cause.[206] Essentially, the entire spectrum of location data, from the suspect's location when he made a single phone call to four months' worth of driving patterns, is governed by the same standard.

---

202 Electronic Communications Privacy Act of 1986, Pub L. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.). Note once again the dominant position that "privacy" has in the popular and political imagination.

203 *See* 18 U.S.C. §§ 2510–2522 (2006).

204 *See id.* § 3123(a)(1).

205 GPS Act, S. 1212, 112th Cong. sec. 2 § 2601(4) (2011).

206 *Id.* sec. 3 (incorporating the warrant standard of Federal Rule of Criminal Procedure 41(d)); *see also* FED. R. CRIM. P. 41(d) (explaining that warrants under the Rule must be issued upon a showing of probable cause).

Thus, the GPS Act puts forth a more demanding standard for law enforcement than even the privacy theory espoused by *Maynard,* which requires only *long-term* data collection to trigger a warrant requirement.[207] This effectively nullifies the advantages of using a limited, "snapshot" level of data collection to help build a case for a more intrusive investigation.[208] If police officers require probable cause to obtain any amount of location data, even the mere confirmation of a suspect's location at a single moment in time, the savings in time and manpower that the data provide are reduced and there is less incentive to rely on this method over physical tactics such as interrogation or obtaining a search warrant for the suspect's home.

The statute seeks to protect a notion of privacy, much like the *Maynard* standard, but trades uncertainty in application for unreasonable burdens on effective police work. More puzzlingly, as a policy rationale, it remains unclear how a single item of location data conveyed to a cell phone company is more "private" than being seen by another person on a public street at the same time, engaged in the same activity. The GPS Act's vision of privacy, converted into its across-the-board rule, bears no more durable relationship to "private" information than the *Maynard* standard does.

A regulatory solution oriented around a different set of goals, that dispenses with protecting privacy as its source of legitimacy and also eschews case-by-case judicial clarification, would limit strategic police behavior by avoiding an amorphous privacy standard like the one contained in the GPS Act, and would avoid Congress' once-every-two-decades approach. But if a regulatory regime were not limiting police behavior or imposing a warrant requirement in the name of individual privacy, that raises the question: what would be its rationale? Part V suggests that the rationale could be preventing the institutional, rather than individual, harm that results from unchecked police discretion.

V. Moving Beyond Privacy: A Theory of Institutional Harm and Its Policy Implications

Privacy arguments are the standard reasons for limiting police investigative behavior,[209] but this emphasis on a difficult-to-define individual right obscures another harm: institutional harm. Unchecked police surveillance and strategic behavior deprive the judiciary of the

---

207 *See supra* Part III.B.

208 *See supra* Part I.A.

209 *See* Kerr, *supra* note 11, at 805.

information and power to ensure that police action is reasonable and that cases are adjudicated based on evidence properly obtained. As Professor David J. Phillips has observed, privacy theories do not account for the way that surveillance technologies shift the balance of power among institutions.[210] The time has come to look beyond individual privacy-based harms to other doctrinal bases for limiting police surveillance.

By analogizing to doctrinal discussions of agency behavior in administrative law, one can observe that unchecked surveillance also produces an institutional, rather than purely individual, harm. Once this type of harm is considered, a different standard for limiting police surveillance emerges: rather than view regulation as being appropriate *only* when a privacy interest is infringed upon, regulating surveillance using some form of warrant requirement should be the norm *unless* a compelling reason renders those mechanisms inappropriate.

A. Post Hoc Rationalization and Unchecked Executive Discretion as an Institutional Harm: Observations from Administrative Law

Outside of the criminal procedure realm, another body of scholarship where post hoc rationalization and judicial review have long been topics of discussion is federal administrative law.[211] This scholarship provides a useful insight: if one thinks of police departments as administrative agencies, such as the Environmental Protection Agency or the Federal Communications Commission, unlike those agencies, many of the police departments' actions directed at private citizens are done without a meaningful contemporaneous record, thereby grossly limiting judicial review.[212]

Of course, important differences exist: federal agencies' actions are reviewed by judges under a set of general minimum standards[213] found in the Administrative Procedure Act,[214] and the closest analogue for police departments and criminal procedure is the Constitu-

---

210 *See* David J. Phillips, *Beyond Privacy: Confronting Locational Surveillance in Wireless Communication*, 8 COMM. L. & POL'Y 1, 1–3 (2003).

211 *See* Jim Rossi, *Antitrust Process and Vertical Deference: Judicial Review of State Regulatory Inaction*, 93 IOWA L. REV. 185, 225 (2007) (noting that judicial concerns about, and refusal to defer to, post hoc rationalizations by agencies justifying their actions is a "foundation of administrative law, frequently serving as a basis for agency reversal" that incentivizes agencies to adequately document their reasoning).

212 *See supra* Part II for a discussion of investigative scenarios where this occurs.

213 *See* 5 U.S.C. § 706 (2006).

214 Administrative Procedure Act, Pub. L. No. 79-404, 20 Stat. 237 (1946) (codified as amended in scattered sections of 5 U.S.C.).

tion. Nonetheless, recent scholarship has found fertile ground in looking to administrative law as a source for inspiration in criminal procedure and law enforcement debates.[215]

Key points of similarity exist between administrative law and criminal procedure: at present, courts defer to police officers' experience and factual determinations in reviewing investigative action in much the same way that they defer to agency factfinding or interpretive decisions.[216] Moreover, much like administrative agencies regulating the companies in a given industry, local police departments undertake actions that have profound effects for private citizens.[217] It is worth considering then that a central issue in administrative law has been judicial concerns about agency post hoc rationalization and its corrosive effect on judicial review.[218]

In reviewing a federal agency's action, even under a deferential "arbitrary and capricious" standard,[219] courts have refused to look beyond the contemporaneous or preexisting record justifying that action. As the Supreme Court articulated in *SEC v. Chenery Corp.*,[220] it is the agency's record laying out its reasoning that is the basis for judicial review;[221] or as the Court phrased it in a later decision, "[t]he courts may not accept appellate counsel's *post hoc* rationalizations for agency action."[222] The implication of that requirement is that, for a reviewing court to evaluate and sustain an agency's action, some record prior to the agency action must exist or else the court risks becoming a rubber stamp for agency decisions.[223] The rationale behind

---

215 *See, e.g.*, Rachel E. Barkow, *Institutional Design and the Policing of Prosecutors: Lessons from Administrative Law*, 61 STAN. L. REV. 869, 873 (2009) (arguing for an administrative law approach to limiting prosecutorial discretion); Dan M. Kahan, *Three Conceptions of Federal Criminal-Lawmaking*, 1 BUFF. CRIM. L. REV. 5, 16–17 (1997) (arguing for an administrative law conception of federal criminal law); Kami Chavis Simmons, *New Governance and the "New Paradigm" of Police Accountability: A Democratic Approach to Police Reform*, 59 CATH. U. L. REV. 373, 400 (2010) (arguing in favor of conceptualizing police departments as administrative agencies); Simon Stern, *Constructive Knowledge, Probable Cause and Administrative Decisionmaking*, 82 NOTRE DAME L. REV. 1085, 1126–27 (2007) (comparing law enforcement agencies to administrative agencies).

216 *See* Fabio Arcila, Jr., *Suspicion and the Protection of Fourth Amendment Values*, 43 TEX. TECH L. REV. 237, 241–42 (2010) (critiquing the tendency of judges in the criminal procedure context to employ a deferential approach to police actions that resembles judicial treatment of administrative agencies).

217 *See* Simmons, *supra* note 215, at 400.

218 *See* Rossi, *supra* note 211, at 225.

219 *See* 5 U.S.C. § 706(2)(A) (2006).

220 SEC v. Chenery Corp., 332 U.S. 194 (1947).

221 *Id.* at 196.

222 Burlington Truck Lines, Inc. v. United States, 371 U.S. 156, 168 (1962).

223 *Id.* at 167.

this limitation is that the institutional power of federal courts is eroded when an agency is free to regulate private parties without judicial oversight, or is free to explain its actions in court but not required to have done so prior to litigation.[224]

It is in the context of judicial review of agency behavior that the dual nature of police departments, as both entities regulated by the courts[225] and regulators of private conduct, becomes an important observation. As Professor Simon Stern has argued, the criminal procedure analogue to the record-creation requirement for administrative agencies, in a limited sense, is the warrant requirement.[226] When police agencies must seek a warrant, they in effect create a record that provides a reviewing court a window into what the proffered justification was before incriminating evidence was discovered pursuant to the warrant.[227] When such a warrant-based record is absent, a reviewing court has access only to the convenient justifications the police and prosecutors choose to offer during litigation[228]—precisely the post hoc rationalizations for agency behavior the Supreme Court has disparaged in the administrative law context. In effect, the warrant requirement forces a justification for surveillance before incriminating evidence is retrieved, thereby preventing arbitrary or discriminatory surveillance policies by law enforcement agencies.

This analogy, viewing local police departments as administrative agencies, suggests that a court suffers a similar decrease in institutional power when the record produced by a warrant is not required. The Administrative Procedure Act forces record creation to preserve judicial review; the warrant requirement serves a similar function, and its absence weakens judicial review of executive action. This is hardly without structural support in the Constitution itself: the text of the

---

224 This concern is perhaps even more evident in the "hard look" doctrine, where reviewing courts scrutinize the records of a federal agency's original stated policy rationales for taking an action *See* Motor Vehicle Mfrs. Ass'n of the United States v. State Farm Mut. Auto. Ins. Co., 463 U.S. 29, 41–42 (1983) (establishing proposition that agency reasoning must link its evidence, its policy, and its action in some cogent way, or else it risks judicial invalidation as being "arbitrary and capricious").

225 *See supra* Part II.A.

226 *See* Stern, *supra* note 215, at 1132–33 (arguing that judicial deference and the development of a reviewable record are features common to both administrative procedures and the warrant requirement under the Fourth Amendment).

227 *See* United States v. Garcia, 474 F.3d 994, 996 (7th Cir. 2007).

228 This is generally likely to take place during a pretrial suppression hearing, where the defendant challenges the constitutionality of a given officer's actions. *See generally* Sundby, *supra* note 65, at 256–64 (discussing the benefits of the exclusionary rule as forcing at least some articulation of why an officer performs a search in a given fashion).

Fourth Amendment suggests a judicial role in supervising law enforcement through its Warrant Clause.[229] One of the original rationales for suppressing evidence obtained in violation of the Fourth Amendment was that admitting the tainted evidence would erode the institutional legitimacy of *the courts*, in addition to harming the individual.[230]

The judicial concern about unchecked executive power is far from a forgotten one, as illustrated by Judge Flaum's concurrence in *United States v. Cuevas-Perez*,[231] an April 2011 Seventh Circuit opinion.[232] In *Cuevas-Perez*, the majority of the panel declined to adopt *Maynard's* approach, following Seventh Circuit precedent and noting the brevity of the tracking in the case.[233] However, Judge Flaum authored a separate concurrence that offers an important alternative insight into the public-conduct surveillance dilemma that *Maynard* attempted to address. Concluding that *Maynard's* theory is unworkable under the *Knotts* precedent,[234] Judge Flaum observed that there may be other reasons to regulate GPS technologies beyond the privacy interests invoked in *Maynard*. These reasons included "that the use of GPS technology to engage in long-term tracking is analogous to general warrants that the Fourth Amendment was designed to curtail, because of the technology's potential to be used arbitrarily."[235] This point, which looks to the problematic lack of a justification for surveillance conducted without a preexisting record, and the potentially destructive effects of unchecked executive discretion, is explored further in the next Section as a doctrinal justification for this Note's proposed framework.

---

229 *See* U.S. CONST. amend. IV; *see also* Elkins v. United States, 364 U.S. 206, 216–17 (1960) (discussing the check that courts must place on law enforcement behavior: "What is here invoked is the Court's supervisory power over the administration of criminal justice in the federal courts").

230 *See Elkins*, 364 U.S. at 222–23.

231 United States v. Cuevas-Perez, 640 F.3d 272 (7th Cir. 2011).

232 *Id.* (Flaum, J., concurring). Professor Orin Kerr has made a conceptually related argument: that judicial interpretations of the Fourth Amendment reflect a desire for equilibrium between citizen freedom and police power; this descriptive theory of Fourth Amendment decisions is thus premised in part on concerns about police agencies as institutions. *See* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 487 (2011) ("Equilibrium-adjustment acts as a correction mechanism. When judges perceive that changing technology or social practice significantly weakens police power to enforce the law, courts adopt lower Fourth Amendment protections for these new circumstances to help restore the status quo ante.").

233 *Cuevas-Perez* 640 F.3d at 275–76.

234 *Id.* at 279–80 (Flaum, J., concurring).

235 *Id.* at 285.

Concern over the erosion of judicial supervisory power is particularly relevant in the present American criminal justice system. More than ninety-five percent of federal felony and class A misdemeanor prosecutions end in plea agreements rather than trials,[236] and the states follow a similar pattern.[237] This trend has the effect of limiting the court's role and making police action, not trial, the primary determinant of who is convicted and sentenced.[238] Pleading guilty necessarily forecloses a meaningful evaluation of the government's behavior and evidence by the court, unless a suppression hearing is conducted prior to the plea. Forcing the creation of a record through a warrant requirement allows for meaningful review of the investigative actions that help produce this vast volume of plea deals, thereby providing a basis for suppression hearings and thus preserving judicial oversight and the institutional power of courts.

Viewing police departments as administrative agencies with power that needs to be checked by judicial review has an important policy implication for surveillance technologies and judicial regulation of the police. The more effective a surveillance tactic is at generating evidence for leveraging a plea or obtaining a conviction at trial, the more that tactic diminishes judicial power if left wholly unsupervised, because the surveillance technology provides for limitless collection of evidence without requiring the government to explain its focus on the particular suspect. Public-conduct surveillance technologies, with their power to create comprehensive, permanent records of citizen behavior,[239] thus present a serious risk of institutional harm: the erosion of judicial oversight of the police.

B. Standards for Regulation Premised on a Theory of Institutional Harm, Rather than Privacy-Based Harm

When one considers the institutional harm posed by the absence of a warrant requirement, it suggests a conceptual shift away from regulating the police in order to preserve some notion of individual pri-

---

236 In fiscal year 2009, 96.3% of felony defendants pleaded guilty in federal district courts. *See* U.S. SENTENCING COMMISSION, 2009 SOURCEBOOK OF FEDERAL SENTENCING STATISTICS tbl.11 (2009), *available at* http://www.ussc.gov/Data_and_Statistics/Annual_Reports_and_Sourcebooks/2009/Table11.pdf.

237 In 2006, 94% of felony defendants pleaded guilty in a sample of state court cases. *See* SEAN ROSENMERKEL ET AL., U.S. DEP'T JUSTICE, FELONY SENTENCES IN STATE COURTS, 2006—STATISTICAL TABLES, 25 tbl.4.1 (2009), *available at* http://bjs.ojp.usdoj.gov/content/pub/pdf/fssc06st.pdf.

238 *See id.*

239 *See supra* Part I.A.

vacy rights. The privacy-centered view presumes that when the police do not violate a citizen's privacy interests, no regulation is needed.[240] But once one considers instead the institutional harm to the courts stemming from investigative conduct that is arbitrary, that generates an extensive evidentiary record, and that is only justified, if at all, after the fact in court, a very different approach becomes needed. The institutional harm takes place when citizens are indicted and plea deals are induced without scrutiny of the evidence. Accordingly, any citizen so indicted should have the ability to challenge evidence supporting the charges, irrespective of whether a personal privacy interest has been violated.

Applying that conceptual shift to public-conduct surveillance thus demands a warrant requirement because the most oft-invoked policy reason for tolerating after-the-fact police explanations for official behavior—safety—is absent. Using a theory of public and officer safety, the Supreme Court has repeatedly justified granting police officers discretion to take action and then allowing them explain the action later. This justification has been invoked in a host of scenarios, from the officer's power to summon drivers out of their cars,[241] to arrest procedures,[242] to warrantless entries of private homes.[243] The dangers inherent in police work demand that officers be accorded the ability to make snap decisions based on limited information. In those contexts, post hoc justification without a preexisting record is a problem that must simply be borne. But in the context of electronic surveillance, that rationale vanishes. There is no meaningful threat to officers or citizens during extensive remote recording of public movements, so a principal justification for broad discretion is removed.[244] Without that justification, the case for tolerating the erosion of judicial regulatory

---

240 *See supra* Part III.

241 *See, e.g.*, Pennsylvania v. Mimms, 434 U.S. 106, 111–12 (1977) (holding that an officer has a per se right to order a driver out of her vehicle to ensure officer safety during investigative or traffic stop); Terry v. Ohio, 392 U.S. 1, 23–24 (1968) (partly justifying stop-and-frisk tactic based on the need to ensure officer's safety during street encounters).

242 *See, e.g.*, New York v. Quarles, 467 U.S. 649, 655–56 (1984) (recognizing "public safety" exception to Miranda warning requirement because of need for officers to react to threats to public safety); Washington v. Chrisman, 455 U.S. 1, 7 (1982) (finding that "[e]very arrest must be presumed to present a risk of danger to the arresting officer," which justifies an officer maintaining close control over arrestees).

243 *See, e.g.*, Brigham City, Utah v. Stuart, 547 U.S. 398, 403–04 (2006) (finding that the need to aid potentially injured residents justified warrantless entry into a home).

244 See text accompanying notes 39–46 for a discussion of the secretive character of GPS surveillance. Obtaining cell phone records or similar data poses even less of a safety concern because the police agents never interact with the suspect in any physical way.

power through unchecked police surveillance becomes much less compelling.

This theory of institutional harm suggests the following general principle: surveillance tactics that generate powerful, permanent evidentiary records should be presumptively governed by a warrant requirement, irrespective of whether they violate a *Katz*-approved privacy interest, and exceptions should be made only when other policy concerns demand it. Although arguably this rationale would extend to a broad swath of nonsurveillance police actions, the safety concerns present in most scenarios where the police physically intervene would counsel against such an outcome.

Combining this conceptual shift away from privacy-centered regulation with the observed reality of how police respond strategically to case-by-case judicial rulemaking,[245] the appropriate mechanism for regulating public tracking technologies becomes more apparent. A set of technology- and use-specific regulations could provide the initial clarity that a slowly evolving and unclear doctrine lacks, and a warrant requirement that does not depend on an ephemeral conception of privacy preserves an institutional check on executive power. It accomplishes this not by preventing surveillance from occurring, but by forcing the creation of an ex ante record that grants the courts insight into the investigative process before monitoring begins.

A natural concern about broadly applying a warrant requirement to public-conduct surveillance might be that it would result in fewer uses of the technology and thus less effective police work. Imposing a warrant requirement, however, does not necessarily result in a tactic being used less often, except in instances where there is simply no basis on which a warrant could be granted. For example, in 2008, there were 1,891 warrant applications to install wiretaps to record electronic or telephonic communications; not one warrant application was denied by a magistrate.[246] The value of the requirement is proven not by the denial of applications, however, but by broad compliance with a rule forcing the creation of ex ante records.

What is needed then is a uniform legal framework for trial-level judges to review the public-conduct surveillance tactics of local police departments. So long as the Fourth Amendment is defined by the outer limits of privacy theories, the Constitution will not reach public-

245 *See supra* Part II.

246 *See* ADMIN. OFFICE U.S. COURTS, APPLICATIONS FOR ORDERS AUTHORIZING OR APPROVING THE INTERCEPTION OF WIRE, ORAL, OR ELECTRONIC COMMUNICATIONS 7 (2009), *available at* http://www.uscourts.gov/uscourts/Statistics/WiretapReports/2008/2008WTText.pdf.

conduct surveillance without paying a price: reduced enforcement efficacy resulting from vague standards and strategic police reactions.[247] What is needed is a kind of Administrative Procedure Act regime for police use of public-conduct surveillance technologies: a permanent agency with a mandate to address new technologies with formal rulemaking that binds police departments uniformly.

VI. An Administrative Solution: Vesting Primary Regulatory Power with an Agency Rather than with Congress

A federal rulemaking regime that regulates all law enforcement use of technologies that comprehensively record a citizen's public conduct would both appropriately limit, or permit, police discretion while avoiding the doctrinal morass of the *Maynard* standard. In constructing such a regime, Congress need only provide a central limiting principle for the regulations and a mandate for action in response to petitions for rulemaking.

Moreover, the regime should employ a grant program that distributes surveillance technologies evenly across the country but imposes a clear warrant requirement. This would give small departments access to the benefits of public-conduct surveillance tactics as crime-fighting tools, while at the same time preventing the institutional harms of strategic police behavior and unchecked surveillance discretion.[248]

In drafting the necessary legislation, Congress should depart from its prior approaches and primarily give a grant of rulemaking authority to an agency that will manage the disbursement of federal funds to state and local law enforcement. This Section argues that the basic elements of this new program should be a grant program administered by an independent agency—a Surveillance Technology Review Board—which would reward states and agencies that comply with and adopt the regulations and deny or reduce funding to those that do not; a regulation-based warrant requirement; and exclusionary remedies and economic penalties in the event the regulations are violated.

---

247 *See supra* Part III.C.

248 *See supra* Part III.C.

A. A Grant Program, Enacted Pursuant to Congress's Spending Power and Administered by a Surveillance Technology Review Board

This new legislation should take the form of a technology grant program with the regulations functioning as the conditions for receipt of the funds. Congress enjoys broad authority under the Constitution to impose conditions upon spending grants to the individual states,[249] provided that Congress make its policy rationale and the conditions imposed clear.[250] As discussed above, the federal government already has an established relationship with state law enforcement agencies as a source of financial support, and such a grant program would be an extension of that trend.[251] Further, this approach is hardly foreign to the current federal government: for example, the Department of Education promulgates regulations that prohibit discrimination in education, and those regulations reach all schools that receive federal financial support under Title IX of the Education Amendments of 1972.[252] This proposed grant program would merely be taking a Title IX approach to surveillance technologies by enhancing the Office of Justice Programs' grant-making powers and making the entity politically independent with the creation of a Surveillance Technology Review Board.

The essential legislative grant of rulemaking power to the Surveillance Technology Review Board would simply be the authority to promulgate regulations that govern any surveillance technology that generates permanent electronic records of private citizens' conduct, with the mandate that the agency must respond to petitions for rulemaking by citizen groups. This general principle would constitute a permissible grant of authority by Congress,[253] and under the Supreme Court's decision in *Massachusetts v. EPA*,[254] would also constitute a clear mandate that the agency act in response to new and evolving surveillance technologies. This mandate would make the agency more responsive to citizen demands for regulation than Con-

---

249 *See* South Dakota v. Dole, 483 U.S. 203, 207–08 (1987) (finding that the only minimal constraints on conditional spending by Congress are that it serve public welfare, relate in some way to the federal interest at stake, and that Congress make the conditional nature of the program clear).

250 *Id.* at 207.

251 *See supra* Part I.B.

252 Title IX, Education Amendments of 1972, 20 U.S.C. §§ 1681–1682 (2006); *see also* 34 C.F.R. § 106 (2010) (effectuating Title IX of the Education Amendments of 1972).

253 *See supra* notes 249–52 and accompanying text.

254 *See* Massachusetts v. EPA, 549 U.S. 497, 532–35 (2007) (holding that the EPA cannot reject a rulemaking petition that is authorized under the Clean Air Act based on arbitrary, capricious, or other reasons not in accordance with the law).

gress's current approach of allowing decades to elapse between reforms.

The program could also facilitate the even distribution of the tracking technologies among law enforcement agencies, provide training for their use, and help address the apparent rural law enforcement technology gap identified in Part I.[255] In addition, the conditional-grant nature of the agency's power would provide states with the ability to make a political decision about their police agencies' independence: they could opt out and maintain their own approach to tracking technologies, but it would come at the expense of federal grants and other material support.[256]

B. A Warrant Requirement

The central provision of this statutory scheme would be the requirement that federal agents and police officers obtain a warrant or court order before securing location data. The standard upon which an order could issue would be set by the Surveillance Technology Review Board's rulemaking, with standards varying according to the technology regulated and the amount of data requested or obtained. Thus, a request for a "snapshot" level of information, such as an electronic tollbooth record or data obtained from a single drone flight, would be granted on a lesser factual showing, while days or weeks of continuous cell-site data would require probable cause.[257] The rationale that explains this spectrum is a need to control executive power and to prevent "fishing expeditions" where monitoring is extensive and originally premised on no more than a hunch. When only a "snapshot" is in play, the police lack the ability to engage in an open-ended analysis of a citizen's behavior; when the data requested spans months, that risk of arbitrary surveillance and selective monitoring becomes a larger concern. The amount of justification required for an order would properly vary based on the extent of the record demanded or obtained by law enforcement officials.

Besides setting a standard that demands specific factual grounds for an officer's belief that tracking a given citizen will lead to evidence of a crime, the probable cause requirement has the benefit of familiarity. Local police agencies have been obtaining warrants on a more or less consistent probable cause standard since 1983, when the Supreme

---

255 *See supra* Part I.A.

256 Further, this would add to the leverage over the states to prevent violations of the regulations. *See supra* Part III.B.

257 Probable cause is the governing standard for the original comprehensive surveillance law, the wiretap statutes. *See* 18 U.S.C. § 2518(3)(a)–(b) (2006).

Court last modified probable cause analysis to embrace "the totality of the circumstances."[258] In contrast, the pen register statutory provisions allow for an order authorizing surveillance to be issued on a showing of mere relevancy to a criminal investigation[259]—a standard that would be appropriate for "snapshot" location data because it is functionally equivalent to obtaining any other evidence that places an individual at a given location at a given moment, such as a receipt from a credit card transaction.

As a policy matter, the volume of information revealed by tracking technology used over a prolonged period makes a mere relevancy standard inappropriate, as such a standard would chiefly block only the most blatantly arbitrary investigative practices.[260] Given that the proposed rationale for regulating public-conduct surveillance tactics is to protect judicial power, probable cause is the preferred standard for any prolonged surveillance because it generates the most robust record for judicial review. The statutory scheme thus would provide a mechanism for forcing presurveillance records and justification, thereby effectively creating an Administrative Procedure Act for surveillance.[261]

C. Exclusion and Economic Penalties for Violation

In order to deter violations of the statute by officers and departments, the empowering statute and the agency regulations should provide for both exclusion of illegally obtained evidence and economic penalties that result in the loss of grant funds.

The provision would first state that no state or federal court could admit into evidence location or other public-conduct data obtained without a valid warrant or similar court order.[262] The exclusion of evidence as a penalty is essential, because it provides the basic deterrent for arbitrary police action: there would be no courtroom success based on the tactic's use unless a warrant or other order was obtained. Such a provision would thus help eliminate the risk of strategic behavior

---

258 *See* Illinois v. Gates, 462 U.S. 213, 237–39 (1983) (rejecting the previous two-pronged probable cause standard as too rigid, adopting instead a totality of the circumstances analysis that traditionally has informed probable cause determinations).

259 *See* 18 U.S.C. § 3123(a)(1).

260 The chief virtue of a higher standard is that it forces government agents to produce a more ample record justifying the need for surveillance, thereby preventing post hoc rationalization, the harm identified in Part V.A.

261 *See supra* notes 211–19 and accompanying text.

262 Similar language can be found within the wiretap legislation. *See* 18 U.S.C. § 2515 (providing for exclusion of evidence obtained outside of the warrant mechanism). Of course, this would only bind the states that accepted the grant conditions.

discussed in Parts II and III, at least insofar as that strategic behavior involved avoiding the warrant requirement for using the technology.

Further, the regulatory board could provide a distinct set of economic penalties for departments that accepted federal funds but nonetheless engaged in warrantless surveillance. A finding that the department had placed citizens under surveillance without court order would trigger a reduction in the funding available to that department, and could be used to affect its eligibility for future grants. Similar grant-reduction penalties could be imposed for failing to maintain appropriate records detailing how the surveillance was conducted.[263]

This approach has a variety of policy virtues over *Maynard's* vision of purely judicial, albeit uncertain, regulation and Congress's proposed overbroad approach. An agency scheme that combines a conditional grant program with regulation-based, data-specific warrant requirements would both avoid the strategic behavior associated with unclear judicial rules and prevent the weakening of judicial power through unchecked executive surveillance capabilities. In the same vein, the use of an administrative regulatory scheme would avoid the one-size-fits-all approach of the current proposed legislation, allowing for a more demanding standard when law enforcement seeks a comprehensive record of public conduct and lesser factual showings for more isolated, "snapshot" requests.

In sum, the proposed warrant requirement established through the regulations would ensure that a record existed to justify police action before surveillance began, guaranteeing informed judicial review over subsequent prosecutions relying on the evidence obtained. Finally, the use of a federal grant program would provide a powerful investigative tool to small and rural agencies that could benefit from a technology that requires little manpower to employ. The regime discussed above would both regulate and assist law enforcement.

CONCLUSION

Although most of the uniform rules applied against local police agencies are judicially enforced and rooted in the Constitution, new surveillance technologies are testing that convention, as well as the limits of privacy as a basis for those rules in the absence of a physical trespass. In attempting to regulate comprehensive tracking technology through the Fourth Amendment, the D.C. Circuit demonstrated

263 The wiretap statutes contemplate a private cause of action for violations, but expressly limit the statutory damages. *See id.* § 2520. A similar private cause of action could be useful for bringing violations to the attention of the federal government, though the emphasis would remain on funding-based reductions and penalties.

how the expansive new standard demanded by privacy advocates would invite the same sort of strategic response seen in other areas of constitutional law. Expanding privacy to expand regulation will lead to uncertainty and reduced efficacy of judicial rules.

Beyond privacy, a more durable regulatory theory can be found: safeguarding judicial power by preventing strategic behavior and after-the-fact justifications for executive action. In that context, inspired by an analogy to administrative law doctrine, imposing a warrant requirement need not depend on whether a given police activity implicates privacy. Forcing police agencies to generate presurveillance records like warrant applications, pursuant to a comprehensive agency-driven regulation regime, should be the preferred method *unless* a compelling interest like officer safety cautions otherwise.

Where the Constitution is neither an effective nor available means to regulate police conduct, Congress has a natural role to play, particularly given the financial bond forged between the federal government and local departments over the last several decades. A grant program—a familiar incentive for state participation—coupled with conditions that impose a warrant requirement on the technologies' use would maintain judicial supervision and limit police discretion, with its attendant strategic behavior.

With a uniform warrant or other record requirement guiding the use of surveillance tactics, a modest but nonetheless valuable advance would take place. Police departments would be more effective at keeping criminal suspects under surveillance, and courts and society at large would have greater confidence that objective evidence justifies the monitoring of specific private citizens. Moreover, the rules adopted by the proposed Surveillance Technology Review Board would not suffer from the arbitrary line-drawing and opportunities for strategic reactions that a *Maynard*-style privacy theory produces, nor would they sweep so broadly as to deny powerful investigative tools to the police.

The above proposals are not without potential drawbacks, but relying on an institutional explanation for why surveillance technologies ought to be regulated has a dramatic advantage over the approaches currently put forth by Congress and the courts: a coherent link between the harm identified and the rule put in place. When one takes the proposed regulatory route, the control of public-conduct monitoring presents a less pernicious legal issue. Freed from trying to apply constitutional protections long associated with homes and personal property to behavior that takes place on public roads, future commentators might conclude that relying on "privacy" was the problem all along.