
RUTGERS LAW REVIEW

VOLUME 65

Summer 2013

NUMBER 4

INTRODUCTION

THE ETERNALLY YOUNG FOURTH AMENDMENT COMMON LAW

*George C. Thomas III**

For more than a century, the Supreme Court has pretended that the text of the Fourth Amendment is instructive on the scope of the protection offered by the amendment. It is time to announce that the emperor has no clothes. The part of the Fourth Amendment that governs the vast majority of cases cannot possibly be instructive as a text. The Court has had to construct a common law from thin air with a dash of history. While there is truth to Akhil Reed Amar's charge that Fourth Amendment doctrine is like "a sinking ocean liner—rudderless and badly off course,"¹ the Court has a pretty good excuse. There is nothing in the first clause of the Fourth Amendment to guide them.²

For reasons lost in the mist of history, the Framers wrote the two clauses of the Fourth Amendment in very different ways. The second clause is framed in clear and specific language: "[N]o Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."³ One can imagine difficulties interpreting "probable cause" but the Framers probably thought the term pretty well spelled out in the common law. The other terms are about as precise as can be found in a constitution.

* Rutgers University Board of Governors Professor of Law and Judge Alexander P. Waugh Sr. Distinguished Scholar, Law School, Newark.

1. Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 759 (1994).

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

3. *Id.*

The first clause, on the other hand, is a hodgepodge of specific and spacious language: “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures shall not be violated”⁴ The right in question applies to “persons, houses, papers, and effects.”⁵ While problems eventually arose in applying those terms, the Framers would have considered the terms quite self-evident and contained.⁶ But the government action that is forbidden is neither self-evident nor contained: “unreasonable searches and seizures.” Leave aside the problem of figuring out the margins of “search” and “seizure”—again, the Framers probably thought the meaning of those words was self-evident—the prohibition of “unreasonable” government action leaves one wondering what the Framers could have been thinking. Like beauty, “reasonable” government action is largely in the eye of the beholder. Why not spell out with more specificity the governmental practices that the Framers wanted to prohibit?

I once tried to work out a more precise Fourth Amendment that would deal adequately with modern threats to privacy and property.⁷ While I like to think the article is a useful addition to Fourth Amendment literature, I confess that my newly-minted “Fourth Amendment” was awkward, cumbersome, and still incomplete. Thomas Davies “solved” the mystery of the radically amorphous “unreasonable searches and seizures” in a very different way—by unearthing historical evidence that “unreasonable” meant unconstitutional.⁸ Viewed that way, the Fourth Amendment says that there shall be no unconstitutional searches and seizures, but that is obviously not very helpful in determining which searches and seizures are “unreasonable” or “unconstitutional.” Perhaps “unconstitutional” is defined by implication in the second clause as any search or seizure not authorized by a specific warrant.⁹ That universe would include all warrantless searches as well as searches pursuant to a general warrant.¹⁰ If this is the right way to view the Fourth Amendment, the reasonableness clause has no independent force; the amendment prohibits only searches not supported by a specific warrant. This is Davies’s conclusion from the historical

4. *Id.*

5. *Id.*

6. See Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 601-08 (2000).

7. See George C. Thomas III, *Time Travel, Hovercrafts, and the Framers: James Madison Sees the Future and Re-Writes the Fourth Amendment*, 80 NOTRE DAME L. REV. 1451 (2005).

8. See Davies, *supra* note 6, at 684-93.

9. See *id.* at 684.

10. See George C. Thomas III, *Stumbling Toward History: The Framers’ Search and Seizure World*, 43 TEX. TECH L. REV. 199, 209 (2011).

evidence.¹¹ Thomas Clancy and William Cuddihy have also delved deeply into the same history, and both embrace the conventional view that the Framers *did* intend the first clause to have independent meaning,¹² that it prohibits a subcategory of warrantless searches and seizures as well as general searches.

History is clear that the major concern of the Framers was general warrants. Once the Framers took care of that problem in the second clause by requiring specific warrants based on probable cause, supported by oath or affirmation,¹³ perhaps they were content to let the common law govern ordinary, run-of-the-mill violations of property and privacy interests. I have argued that the reference to “unreasonable searches and seizures” referred to the common-law tort of trespass, which had protected privacy and property in England and America for centuries.¹⁴ This view neatly explains why there is no remedy spelled out in the amendment.¹⁵ Tort law provided both the right and the remedy for run-of-the-mill violations of privacy and property rights.¹⁶ Indeed, it was not until 1914 that the Supreme Court began to fashion a remedy for violations by individual officers, as opposed to statutes that ran afoul of the Fourth Amendment.¹⁷ Clancy and Cuddihy respond that there is evidence of colonial concerns that go beyond general searches.¹⁸ Even if general searches were the principal concern of the Framers, they could also have intended the first clause to regulate routine searches and seizures that violated privacy and property. True enough.

The historical debate over why the Framers wrote the Fourth Amendment the way they did is unlikely ever to be settled. But there can be little doubt that the text of the first clause¹⁹ is unhelpful, at least standing alone. Perhaps the Framers intended not merely to

11. See Davies, *supra* note 6, at 551.

12. See Thomas K. Clancy, *The Framers' Intent: John Adams, His Era, and the Fourth Amendment*, 86 IND. L.J. 979, 983 (2011); WILLIAM J. CUDDIHY, *The Emergence of the Fourth Amendment, 1776-1791*, in THE FOURTH AMENDMENT: ORIGINS AND ORIGINAL MEANING, 602-1791, 1359, 1403-14 (UMI Dissertation Services 1997).

13. U.S. CONST. amend. IV.

14. See Thomas, *supra* note 10, at 219-25.

15. See *id.* at 215-18.

16. See *id.* at 209.

17. Compare *Weeks v. United States*, 232 U.S. 383, 398 (1914) (holding that evidence seized by an individual officer in violation of the Fourth Amendment must be returned to its owner) with *Ex parte Jackson*, 96 U.S. 727, 730 (1877) (considering whether a federal statute prohibiting putting certain items in the U.S. mail violated the Fourth Amendment). To be sure, the Court relies, in part, on the Fourth Amendment in the habeas case involving two defendants implicated in the Aaron Burr conspiracy. See *Ex parte Bollman*, 8 U.S. (4 Cranch) 75 (1807). But the issue there was the legality of the detention, not a search or seizure.

18. See Clancy, *supra* note 12, at 1027-29; CUDDIHY, *supra* note 12, at 454-58.

19. U.S. CONST. amend. IV.

reference the common law of trespass, but to embed it into the Fourth Amendment. Courts interpreting the Fourth Amendment could then find its meaning in the common law. That raises all sorts of questions about whether the Framers intended to embed the common law as it existed in 1791 or as it evolved over time. Luckily, those questions do not have to be settled for me to make my larger point. Even if the Framers did not intend to embed the common law of trespass in “unreasonable searches and seizures,” the open-ended nature of the formulation has required the Court to create out of whole cloth the scope of Fourth Amendment protection, just as earlier courts created the common law. As Warren and Brandeis put it in their famous 1890 Harvard Law Review article about the right to privacy: “Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society.”²⁰

In sum, whatever the Framers intended, and whatever a “common law of the Fourth Amendment” means in a technical sense, the open-ended nature of the scope of the right has required the Supreme Court to fashion, and re-fashion, the Fourth Amendment to meet evolving challenges to privacy and property. The Supreme Court has done for the Fourth Amendment what English and American common law courts did for tort law when the Court reasons from case to case to create a meaning of “unreasonable searches and seizures.”

As this symposium demonstrates, the task of creating meaning for “unreasonable searches and seizures” has grown ever more daunting as technology becomes more invasive and more ubiquitous in a world plagued by terrorism. The common law of trespass, adequate for threats to privacy and property in the eighteenth century, would be at a loss to address the issues contained in the articles in this issue. Had the Framers specifically embedded the 1791 common-law trespass right as the meaning of “unreasonable searches and seizures,” the issues raised here would have to be resolved by statute. But the principles that the common-law tort of trespass reflected can shed light on the evolving common law of “unreasonable searches and seizures.” In answering the question of whether an individual has a weapon to use to protect his privacy, Warren and Brandeis wrote: “It is believed that the common law provides him with one, forged in the slow fire of the centuries, and today fitly tempered to his hand.”²¹ The same applies to the Fourth Amendment.

The Fourth Amendment must continue to evolve to be “fitly

20. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

21. *Id.* at 220.

tempered” to a 2013 world.²² Consider Clifford Fishman’s article, *Searching Cell Phones After Arrest: Exceptions to the Warrant and Probable Cause Requirements*.²³ Fishman argues that the exigent circumstance to the warrant requirement (and sometimes to the probable cause requirement) can be applied in a relatively straightforward manner to searches of cell phones. So, for example, the police arrest a suspect for selling narcotics and seize his cell phone. If it rings while police are transporting the suspect to the police station, it would seem that police have grounds to answer the call and get the number of the caller on the basis of probable cause to believe that the call is drug related. The exigency is that the “incoming call would . . . disappear[]” if not answered.²⁴

That example is straightforward enough, but Fishman also has to deal with the problem of searching the stored memory of the cell phone. That exigent circumstance problem is a new one created by technological advances. One rationale allowing a search of cell phone memory is that later messages might exceed the storage capacity of the phone and thus erase earlier messages that might be relevant to the investigation. But, as Fishman points out, the vast storage capacity on new phones has made that rationale already outdated.²⁵ A new problem has arisen: It is apparently possible to erase a cell phone’s memory remotely. Fishman discusses several reasons why this might not be sufficient to trigger the search of the cell phone’s memory without a warrant.²⁶ But my point is: How would a court tease this doctrinal web from the prohibition of unreasonable searches and seizures? The answer is that “unreasonable searches and seizures” has meaning only through the evolving common law of reasonableness “fitly tempered” to the hand of the judge making the decision.²⁷

A more glaring example of how cell phones create havoc for the Fourth Amendment common law is the search incident to arrest exception to the warrant requirement. As Fishman points out, this is a relatively stable doctrine outside the cell phone context. Police can search an arrestee’s person and any objects found on his person, without regard to whether they have probable cause to make the search.²⁸ But, as Fishman points out, these cases were “decided years or decades before the smart phone era [and] do not and could not have taken into account the technological advancements that make a

22. *Id.*

23. *See infra* Clifford Fishman, *Searching Cell Phones After Arrest: Exceptions to the Warrant and Probable Cause Requirements*, 66 RUTGERS L. REV. 995 (2013).

24. *Id.* at 1005.

25. *Id.* at 1008-09.

26. *Id.* at 1009-11.

27. *See* Warren & Brandeis, *supra* note 20, at 220.

28. *See* Fishman, *supra* note 23, at 1013.

modern cell phone the repository of huge quantities of information about its possessor.”²⁹ Thus, the Fourth Amendment common law must evolve again to take account of technological advances. Fishman sketches various ways the incident to arrest exception can evolve where smart phones are involved.³⁰

An even greater challenge to the evolving Fourth Amendment common law is the prospect of 24/7 tracking via GPS or cell phones. Jeffrey Rosen, in *Translating Brandeis’s Right to Privacy in an Electronic Age*, concludes that the Court’s current Fourth Amendment doctrine would not prevent the government from conducting 24/7 electronic surveillance of all movements in public by cell phone or GPS.³¹ I agree. The Court has steadfastly held that movements in public do not implicate the Fourth Amendment.³² In *United States v. Knotts*, the Court held that someone who purchases a can of ether to which a beeper has been attached with the permission of the seller has no Fourth Amendment claim when police use the beeper to track the movement of the can to the defendant’s front yard.³³ The underlying notion is that the Fourth Amendment protects only those activities in which we have a “reasonable expectation of privacy,” a test drawn from *Katz v. United States*,³⁴ and that someone driving on a public road has no reasonable expectation of privacy in his route.³⁵

To be sure, *United States v. Jones* recently held that the Fourth Amendment protects public movements preceded by a trespass that allows the movements to be monitored.³⁶ In *Jones*, the government attached a GPS device to the defendant’s car and used it to monitor his movements for a month.³⁷ The Court unanimously viewed the chain of events as requiring compliance with the Fourth Amendment, though only five members joined Justice Scalia’s majority opinion.³⁸ Scalia sought to draw guidance from the common-law tort of trespass, concluding that attaching the GPS device to the defendant’s private property was a trespass and using the GPS to obtain information about his movements thus implicated the Fourth

29. *Id.*

30. *Id.* at 1015-40.

31. *See infra* Jeffrey Rosen, Keynote Address at the Rutgers Law Review Symposium: Where There is No Darkness: Technology and the Future of Privacy (Mar. 29, 2013), in 66 RUTGERS L. REV. 965 (2013).

32. *See United States v. Knotts*, 460 U.S. 276, 281 (1983).

33. *Id.* at 282.

34. 389 U.S. 347, 360 (1967).

35. *See Knotts*, 460 U.S. at 281.

36. 132 S. Ct. 945, 959-61 (2012).

37. *See id.* at 948.

38. *See id.* at 949.

Amendment.³⁹ Under this theory, the protection of property exists as an add-on protection when the “reasonable expectation of privacy” test fails to suggest Fourth Amendment protection.⁴⁰

The difference between *Jones* and *Knotts*, of course, is the initial intrusion onto the suspect’s property. In *Knotts*, the suspect purchased the can with the beeper already attached.⁴¹ But in *Jones*, Justice Alito, concurring in the judgment and writing for four members of the Court, viewed the initial intrusion as insignificant to distinguish *Knotts*.⁴² Indeed, as we will shortly see, he ridiculed Justice Scalia’s suggestion that the common-law trespass rule would be implicated by what happened in *Jones*.⁴³ For Alito and four members of the Court, what distinguishes the beeper cases is the extent of the surveillance in *Jones*.⁴⁴ It is one kind of violation of privacy to use a beeper to follow someone on a single trip. It is an altogether different violation of privacy to monitor someone’s movements for a month. Stated differently, one might not be surprised to learn that police were following him on a single trip. But one would be stunned to learn that police had monitored all movements of a vehicle for a month.

There is something intuitively appealing in Alito’s approach, which would free the Court to apply the *Jones* principle to forms of electronic monitoring that do not involve a physical trespass, such as the monitoring of GPS devices that were already installed on vehicles as well as cell phone signals. But a moment’s reflection shows how this distorts the holding in *Knotts*. In *Knotts*, the police used the beeper to follow Knotts from Minneapolis to Shell Lake, Wisconsin, a distance of 105 miles.⁴⁵ Can we really say that a driver would not be surprised if police followed him over 100 miles from one state to the next?

Perhaps *Knotts* has been undermined by *Jones*. Maybe there is now a “short trip” rule where the Fourth Amendment does not apply. Justice Alito suggests as much when he writes that “relatively short-term monitoring of a person’s movements on public streets accords with expectations of privacy that our society has recognized as reasonable.”⁴⁶ But what constitutes “relatively short-term monitoring?” There is another “reasonable expectation” problem

39. *See id.* at 949-50; *see also* United States v. Karo, 468 U.S. 705, 714 (1984) (holding that while movements in public were not protected, learning the location of the beeper inside a house *did* implicate the Fourth Amendment).

40. *Jones*, 132 S. Ct. at 951.

41. 460 U.S. 276, 278 (1983).

42. *Jones*, 132 S. Ct. at 958 (Alito, J., concurring).

43. *See id.* at 958-60.

44. *See id.* at 961-62.

45. *See* 460 U.S. at 278-79.

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

highlighted by Justice Sotomayor. She joined the majority's trespass analysis but added a concurrence that raised the third-party doctrine.⁴⁷ The Court has held in numerous cases that when one discloses information to a third party, it is no longer protected by the Fourth Amendment.⁴⁸ Thus, when you dial your telephone, the numbers you dial are transmitted to the phone company and are not protected.⁴⁹ When you disclose financial information to your bank, you have lost Fourth Amendment protection in that information even if you very much want the information to be private.⁵⁰ Your GPS signals are transmitted to a third party and thus are not within your reasonable expectation of privacy as the Court has understood it to date.⁵¹ These cases have always struck me as wrong. To disclose private financial information to my bank is not to disclose it to the world. Indeed, soon after the bank case, Congress provided statutory protection for bank records in the appropriately named Right to Financial Privacy Act of 1978.⁵² But in the absence of a statute, the third-party doctrine would allow police to request GPS locational data from third-party providers. Justice Sotomayor suggested that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."⁵³

Jeff Rosen leads us on a search for an understanding of the Fourth Amendment that provides a better metric for measuring its protections than the "reasonable expectation of privacy" doctrine the Court has used for the last fifty years.⁵⁴ He finds the answer in a place that should not surprise us: Justice Brandeis's dissent in *Olmstead v. United States*.⁵⁵ As Rosen points out, this famous opinion is both amazingly prescient and more soundly grounded in Fourth Amendment values than the mechanical majority opinion in *Olmstead*.⁵⁶ The issue was whether tapping phone lines outside the defendant's home trespassed on his Fourth Amendment rights.⁵⁷ The majority held that the lack of an intrusion onto the defendant's property defeated his Fourth Amendment claim.⁵⁸ In a far-ranging

47. *See id.* at 954-57 (Sotomayor, J., concurring).

48. *See, e.g.,* *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979).

49. *See id.* at 744.

50. *See United States v. Miller*, 425 U.S. 435, 443 (1976).

51. *See Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring).

52. *See* Right to Financial Privacy Act of 1978 (RFPA), 12 U.S.C. §§ 3401-20, 3422 (2006).

53. *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring).

54. *See Rosen, supra* note 31.

55. 277 U.S. 438, 471-85 (1928) (Brandeis, J., dissenting).

56. *See Rosen, supra* note 31, at 973.

57. *See Olmstead*, 277 U.S. at 455 (Brandeis, J., dissenting).

58. *Id.* at 463-64.

dissent that predicted many of the modern technological innovations, Justice Brandeis concluded that the Fourth and Fifth Amendments

conferred, as against the government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.⁵⁹

So rather than “reasonable expectation of privacy” as a definition of what the Fourth Amendment protects, Brandeis and Rosen read the Fourth Amendment to forbid “unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed.”⁶⁰

The Brandeis/Rosen metric is, I think, better than “reasonable expectation of privacy” in three ways. First, the focus is on what the government *does* rather than what a citizen *expects*. The change in focus is appropriate for a protection that seeks to rein in government power. More importantly, the changed focus solves the third-party problem in one elegant stroke. The right question to ask under the Brandeis/Rosen test is not whether one has shared information with a third party, but whether the government has made an unjustifiable intrusion on one’s privacy. I believe if that were the question the Court asked in the bank records case, for example, the result would have been that the Fourth Amendment protects bank records.

Second, putting the focus on the government’s conduct requires the Court to consider what privacy is worth protecting. As the Court has conceded, to phrase the Fourth Amendment’s protection in terms of what society is prepared to recognize as a legitimate expectation of privacy could be abused by government: “[I]f the Government were suddenly to announce on nationwide television that all homes henceforth would be subject to warrantless entry, individuals thereafter might not in fact entertain any actual expectation of privacy regarding their homes, papers, and effects.”⁶¹ Having recognized the problem, the Court offered little in the way of a solution, noting only that “a normative inquiry would be proper” in those cases.⁶² But why not make a normative inquiry in all cases? I think that is what Brandeis is inviting the Court to do when he speaks of unjustifiable intrusions upon privacy.⁶³

Third, the “whatever the means employed” in the Brandeis

59. *Id.* at 478-79.

60. *Id.* at 478; Rosen, *supra* note 31, at 975.

61. *Smith v. Maryland*, 442 U.S. 735, 740 n.5 (1979).

62. *Id.*

63. *Olmstead*, 277 U.S. at 478 (Brandeis, J., dissenting).

formulation⁶⁴ suggests that in *Jones*, Alito was right, that there was no reason to require an initial trespass to find that the intrusion was an unjustifiable one.⁶⁵ On this view, GPS tracking should be treated the same whether the unit was placed on the vehicle by the police or came with the vehicle. And that means that other forms of surveillance that do not require an initial trespass could implicate the Fourth Amendment if sufficiently intrusive.

Scalia's opinion in *Jones* is a creative use of common law to reach a result that seems normatively correct to me and, more importantly, to all nine members of the Court.⁶⁶ But Rosen's contribution to this symposium makes plain that the Fourth Amendment cannot be yoked to the common law. As much as Justice Scalia would like to avoid making normative judgments about what the Fourth Amendment should protect, in the final analysis the Court is going to have to wrestle with the judgments that are implicit in Alito's concurrence in *Jones*.

Bryan Cunningham further demonstrates the difficulty of using the common law of trespass to solve the modern "unreasonable search and seizure" interpretational puzzle. In *Tiny Constables in the Mosaic: Modernizing Oversight of Surveillance in the Age of Big Data*,⁶⁷ the "tiny constables" part of the title comes from Justice Alito's rejection of Justice Scalia's attempt to rely on common law in *Jones*.⁶⁸ Scalia stressed that the initial trespass on the car would have been a tort at common law and the exploitation of that trespass violated the Fourth Amendment.⁶⁹ Seeking to rebut Justice Alito's claim that this kind of trespass would not have occurred in colonial days, Scalia posited a constable who hid in a coach and tracked its movements.⁷⁰ Alito responded that it would have taken either "a gigantic coach or a very tiny constable or both."⁷¹

I agree with Cunningham that it is not beyond the pale to imagine agents of the Crown engaged in surreptitious surveillance of suspected traitors in the colonies.⁷² But if there is any contemporaneous reference to that kind of surveillance being the tort of trespass, I have not seen it. Scalia's imaginative use of the "tiny

64. *Id.*

65. *United States v. Jones*, 132 S. Ct. 945, 959 (2012) (Alito, J., concurring).

66. *See id.* at 948-54.

67. *See infra* Bryan Cunningham, *Tiny Constables in the Mosaic: Modernizing Oversight of Surveillance in the Age of Big Data*, Speech at the Rutgers Law Review Symposium: Where There is No Darkness: Technology and the Future of Privacy (Mar. 29, 2013), in 66 RUTGERS L. REV. 983 (2013).

68. *Jones*, 132 S. Ct. at 958 (Alito, J., concurring).

69. *See id.* at 952.

70. *See id.* 950 n.3.

71. *Id.* at 958 n.3.

72. *See* Cunningham, *supra* note 67, at 986-87.

constable” is, it strikes me, a salutary way to develop a modern common law of “unreasonable search and seizure,” but I agree with Alito that it has no firm basis in the common law as it existed in the colonies.⁷³

If *Jones* is limited to surveillance based on an initial trespass, it does not offer much protection in the world shaped by modern technology and terrorism. Tracking by GPS and cell phone signals involves no trespass. Moreover, as cyberattacks increase in volume and speed, they constitute a greater and greater threat to national security. What role will warrants play in this world? Cunningham concludes that “the traditional methods of judicial oversight—the issuing of individual warrants or orders based on particularity in advance—unfortunately is just not going to be sustainable.”⁷⁴ Another example is the development of the Foreign Intelligence and Surveillance Act⁷⁵ (FISA) courts in response to the need to monitor suspected terrorists without putting them on notice. These courts operate largely in secret—even the names of the judges who review requests to conduct electronic surveillance on suspected terrorists are not public. While Cunningham concedes that the secret nature of the FISA courts is generally appropriate, and I agree, he is concerned that there is no traditional method to test the constitutionality of the FISA statute.⁷⁶ When the ACLU and others challenged the constitutionality of recent amendments to FISA, the Court held in *Clapper v. Amnesty International USA*⁷⁷ that they lacked standing to bring the suit because the plaintiffs could not prove that they had been surveilled. But this of course is a classic Catch-22: Suits to challenge secret surveillance cannot be challenged because the surveillance is secret!

Cunningham does not despair. Indeed, he conscripts his “tiny constables” to retool judicial oversight for the twenty-first century. I leave the details to his excellent presentation, but in sum Cunningham’s “tiny constables” are various technological tools that can oversee the government’s collection of information and send up a red flag when it has exceeded whatever limits exist by statute.⁷⁸ Moreover, Cunningham’s “mosaic” theory provides a potential Fourth Amendment limitation on the amount of information that the government can collect, analyze, and use. In his words, “though particular government intrusions individually may not implicate the Fourth Amendment, when put together, enough of them together, on

73. See *Jones*, 132 S. Ct. at 950 n.3 (Alito, J., concurring). But see *id.* at 958 n.3.

74. See Cunningham, *supra* note 67, at 990.

75. 50 U.S.C. §§ 1801-1871.

76. See Cunningham, *supra* note 67, at 988-89.

77. 132 S. Ct. 1138, 1155 (2013).

78. See Cunningham, *supra* note 67, at 991.

the collection side, which is explicitly what *Jones* deals with, but also on the analysis and use side, may result in the need for judicial scrutiny under the Fourth Amendment.”⁷⁹ And once again, his “tiny constables”—emerging forms of technology—can “track everything the government’s doing with data: what they’re pulling together, what they’re connecting, what they’re distributing, and to better be able to understand where the line might be crossed requiring a warrant or other Fourth Amendment protections.”⁸⁰

Anne McKenna’s article, *Pass Parallel Privacy Standards or Privacy Perishes*, focuses on what in one sense is an even greater problem than the Fourth Amendment’s inability to protect privacy in the twenty-first century.⁸¹ Private businesses, which are not regulated by the Fourth Amendment, are tracking our every movement in physical space as well as in the electronic space. I recently read the novel *Feed* by M.T. Anderson, which imagines a world where the web is implanted in our heads at birth and we are constantly bombarded with advertisements based on what we had bought and sites we had visited.⁸² Before I read McKenna’s article I thought we were well on our way to the *Feed* world. But McKenna’s article makes plain that, except for physically implanting the web in our heads, we are *already* in the dystopian world Anderson imagines.⁸³ The companies Kraft and Adidas plan to “use in-store digital signs equipped with face recognition cameras to target ads specifically for the customer walking near the sign.”⁸⁴ While the current plan is apparently to determine the age and demographics of the person to decide which ads to send to his or her mobile device, McKenna tells us that Google and Facebook “have already begun gathering, storing, and using hundreds of millions of users’ facial biometrics.”⁸⁵ It would be a simple matter to purchase from Google or Facebook access to facial biometrics and know that George Thomas or Anne McKenna is roaming around a Kraft store, and the store could then send ads dedicated specifically to us. (If they hope to send me a text message in the store, well, that is not going to happen but they surely are targeting younger shoppers in any event.)

In addition to facial biometrics, modern GPS systems and mobile devices permit businesses (or government for that matter) to conduct surveillance that is active tracking (real-time) or passive tracking (locating someone’s current location). Both forms of tracking would

79. *Id.* at 993 (internal citation omitted).

80. *Id.*

81. See *infra* Anne T. McKenna, *Pass Parallel Privacy Standards or Privacy Perishes*, 66 RUTGERS L. REV. 1041 (2013).

82. See M.T. ANDERSON, *FEED* (2002).

83. See *id.*

84. McKenna, *supra* note 81, at 1080.

85. *Id.* at 1067.

include, I assume, knowledge of when I'm in my home as opposed to out in public. Active and passive tracking creates many issues. If a government entity does it, we are back to the question of how far *Jones* goes in protecting against this kind of surveillance. And the answer, I think, still is that unless Sotomayor and Alito can find a fifth vote, *Jones* does not circumscribe the ability of government to do active or passive tracking in the absence of a trespass. The third-party doctrine is alive and well. Like Sotomayor, McKenna calls for the third-party doctrine to be abandoned in light of all the entities to which we currently disclose private or semi-private information.⁸⁶ But until that happens, the lack of trespass means that the government can track us via GPS and our mobile devices.

What should we do about the private companies—the Krafts, Adidas, Facebooks, Googles of the world—who want private information not to prosecute us but to make customers of us? To be sure, perhaps because I grew up in a different world, none of this non-government tracking concerns me. I assume when I send an email or visit a web site that I am disclosing that to the world. When I walk in a store, I assume someone might be watching to make sure I don't shoplift. I grew up in a world that had party-line phone service. Several houses used the same line; you knew someone else was using the phone only by picking up the receiver and, necessarily, hearing at least a little of the conversation. If you wanted, you could listen to it all, though the other parties might be aware that you had not hung up the receiver.

I understand that some people do not share my lack of concern about their physical and electronic "movements" where private companies are concerned. As McKenna points out, the European Union tackled the problem of the privacy of personal data almost twenty years ago.⁸⁷ The principles underlying this 1995 statute include notice that the data is being collected, the purpose for which it is collected, a prohibition of disclosure to third parties without consent, access to the information, and redress for violations of the statute. McKenna demonstrates that, in this country, the tentative congressional moves toward protecting privacy are so far outdated and inadequate. She does not attempt a statute that would deal with all these threats to privacy from non-government actors. Such a statute would be amazingly complex. But she does propose a sensible framework that could be used as a starting point for a comprehensive statute.⁸⁸ Will Congress take up this challenge? Forgive me if I am skeptical.

86. *United States v. Jones*, 132 S. Ct. 945, 954-57 (2012) (Sotomayor, J., concurring); McKenna, *supra* note 81, at 1094.

87. *See* McKenna, *supra* note 81, at 1082-84.

88. *See id.* at 1086-92.

Whatever else we can say about the Fourth Amendment, whatever else we can say about what the Framers might have meant, the meaning of “unreasonable searches and seizures” must be constructed as an evolving common law. And the speeches and articles in this symposium make clear that, in the absence of legislation, we should be grateful for the “eternally young” Fourth Amendment common law, “forged in the slow fire of the centuries, and to-day fitly tempered to” to the task of protecting privacy.”⁸⁹

89. Warren & Brandeis, *supra* note 20, at 220.