A COLLECTIVE RIGHT TO BE SECURE FROM UNREASONABLE TRACKING

David Gray[*]

I. INTRODUCTION

> *"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated; and no Warrants shall issue but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."*[1]

In 1983, the Supreme Court confronted the question whether police tracking of a suspect's movements through public space using a radio beeper tracking device constituted a search under the Fourth Amendment.[2] Without dissent, the Court in *United States v. Knotts* held that it did not.[3] According to the Court's reasoning, we expose our movements and activities in public spaces to public view.[4] Accordingly, we have no reasonable expectations of privacy in these movements or activities.[5] It follows that law enforcement

---

* Professor of Law, University of Maryland, Francis King Carey School of Law. My thanks to Arnold Loewy for the invitation to attend the Ninth Annual Criminal Law Symposium at Texas Tech University School of Law and to the editors of the *Texas Tech Law Review* for hosting a wonderful event. I would also like to thank Miriam Baer, Danielle Citron, Jennifer Daskal, Joshua Fairfield, Susan Freiwald, Stephen Henderson, Orin Kerr, Richard McAdams, Richard Myers, Brian Owsley, Margaret Hu, Christopher Slobogin, Judge Stephen Smith, and Stephen Vladeck, each of whom provided invaluable feedback. I am also in debt to those who commented on this work during presentations at Georgetown, the Law and Economics Center at George Mason University, the annual meeting of the Southeastern Association of Law Schools, New England Law, Washington & Lee, and New York University School of Law.

1. U.S. CONST. amend. IV.
2. United States v. Knotts, 460 U.S. 276, 277–80 (1983).
3. *Id.* at 285.
4. *Id.* at 281–82.
5. *Id.* at 282.

officers can observe our persons, our houses, our papers, and our effects from a lawful vantage without implicating the Fourth Amendment.[6]

Although the beeper tracking device used in *Knotts* made it easier for the investigating officers to conduct surveillance with fewer personnel and with less danger of detection, the Court failed to see how technologically enhanced efficiency could raise any additional Fourth Amendment concerns.[7] The technology did not reveal any more information than was already made public.[8] In the Court's view, use of the beeper, therefore, did not raise the stakes for reasonable expectations of privacy.[9] On the other hand, the device enhanced the investigating officers' ability to pursue legitimate law enforcement interests in detecting, preventing, and prosecuting crime.[10] On balance, the Court held, use of the device to aid public surveillance was entirely reasonable from a Fourth Amendment point of view.[11]

According to the *Knotts* Court, attorneys for Knotts caviled but little with its basic analysis.[12] Instead, they focused their objections on the possibility that leaving the use of beeper tracking technology to the unfettered discretion of government agents would license broad and indiscriminate surveillance policies capable of "twenty-four hour surveillance of any citizen . . . without judicial knowledge or supervision."[13] The Court was not unmindful of these threats in the abstract, but nevertheless demurred, reserving the right "to determine whether different constitutional principles may be applicable" should "such dragnet-type law enforcement practices as respondent envisions . . . eventually occur."[14]

Then-contemporary commentators warned about the dangers of the Court's holding in *Knotts*.[15] They were particularly critical of the Court's failure to lay any doctrinal groundwork for assessing and constraining potential government abuse of beepers and other tracking technologies to facilitate programs of broad and indiscriminate surveillance.[16] Those warnings have turned out to be prescient. Although the technical and

---

6. *Id.* at 282–83; *see also* Florida v. Riley, 488 U.S. 445, 451–52 (1989) (holding that anything visible at four hundred feet in the air is open to public view); California v. Greenwood, 486 U.S. 35, 43–44 (1988) (holding that garbage cans left out for collection are open to public rummaging); California v. Ciraolo, 476 U.S. 207, 215 (1986) (holding that anything visible from public airspace is open to public view).

7. *Knotts*, 460 U.S. at 284.

8. *Id.* at 282–83, 285.

9. *Id.* at 285.

10. *Id.*

11. *Id.*

12. *Id.* at 283.

13. *Id.* (quoting Brief for Respondent at 9, *Knotts*, 460 U.S. 276 (No. 81-1802)).

14. *Id.* at 284.

15. *See, e.g.*, Richard H. McAdams, Note, *Tying Privacy in* Knotts*: Beeper Monitoring and Collective Fourth Amendment Rights*, 71 VA. L. REV. 297, 316 (1985).

16. *Id*. at 332–35.

practical limitations of beeper tracking technology made it unsuitable as a tool for mass surveillance, newer technologies have no such limitations.[17] As examples, tracking with the assistance of GPS-enabled devices—whether those devices are planted by law enforcement or are native to our personal technologies—cell-site location, radio frequency identification device (RFID) tags, and the increasingly dense archipelago of surveillance cameras—many of which are linked through computer networks and monitored using a variety of algorithms—have overcome the limits of cost, scale, and human labor that allowed most of us, most of the time, to be secure in the belief that we were not being tracked by radio beepers.[18] In short, the day forestalled by the Court in *Knotts* has come. The question set aside then is before us today: What, if any, "different constitutional principles" should apply to these new and emerging tracking technologies?[19]

This Article argues that contemporary tracking technologies threaten the collective security of the people from unreasonable searches.[20] Some form of Fourth Amendment regulation therefore is necessary. As Danielle Citron and I have argued elsewhere, the best way to provide for the security of the people against the threat of unreasonable searches using contemporary and emerging tracking technologies is to focus on the technologies themselves.[21] Under this technology-centered approach, courts, legislatures, and executive agents would assess the potential of tracking technologies to facilitate programs of broad and indiscriminate surveillance characteristic of a surveillance state.[22] They would then develop and enforce regulatory frameworks sufficient to restore the security of the people by imposing prospective constraints on the deployment and use of tracking technologies with the goal of guaranteeing that most of us, most of the time, are not subject to government tracking.[23]

The argument proceeds in three parts. Part II reviews some of the contemporary and emerging tracking technologies to describe how granting law enforcement officers unfettered discretion to deploy and use these

---

17. David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 Minn. L. Rev. 62, 132–33 (2013).

18. *Id.* at 63–67, 132–33.

19. *Knotts*, 460 U.S. at 284.

20. *See infra* Part II.

21. *E.g.*, Gray & Citron, *supra* note 17, at 63–67, 132–33; *see* Danielle Keats Citron & David Gray, *Addressing the Harm of Total Surveillance: A Reply to Professor Neil Richards*, 126 HARV. L. REV. F. 262, 265–69 (2013) [hereinafter Citron & Gray, *Addressing the Harm*]; David Gray & Danielle Keats Citron, *A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy*, 14 N.C. J.L. & TECH. 381, 391 (2013) [hereinafter Gray & Citron, *Shattered Looking Glass*]; David Gray, Danielle Keats Citron & Liz Clark Rinehart, *Fighting Cybercrime After* United States v. Jones, 103 J. CRIM. L. & CRIMINOLOGY 745, 784–88 (2013).

22. Gray & Citron, *supra* note 17, at 101.

23. *Id*. at 101–02, 111; *see also* David C. Gray, *Fourth Amendment Remedies as Rights: The Warrant Requirement*, 96 B.U. L. REV. (forthcoming 2016), papers.ssrn.com/sol3/papers.cfm?abstract_id=2588739 (discussing how to balance individual privacy interests with modern police tracking capabilities).

devices would leave the people insecure against threats of broad and indiscriminate surveillance. Part III outlines the constitutional principles that should be applied when deciding how the deployment and use of these technologies should be regulated under the Fourth Amendment. Part IV applies these principles to the tracking technologies described in Part II. Part V concludes.

II. CONTEMPORARY TRACKING TECHNOLOGIES

Although law enforcement and other government agents have been developing and deploying a range of evermore sophisticated tracking technologies for several decades, few citizens were aware of their potential to facilitate broad and indiscriminate surveillance.[24] That all began to change in 2012 with the Supreme Court's decision in *United States v. Jones*.[25] In that case, a joint task force of federal and local law enforcement agents investigated Jones's involvement in a narcotics conspiracy.[26] During the course of their investigation, officers sought and received warrants that allowed them to attach a GPS-enabled tracking device to Jones's car and to monitor his movement on public streets.[27] The officers violated the terms of their warrant when they installed the device.[28] They nevertheless used it to track Jones for twenty-eight days, amassing a detailed account of his travels during that time.[29]

Based on the officers' failure to abide by the terms of their warrant, Jones moved at trial to suppress all evidence discovered by or through the GPS device.[30] The trial court, relying on *United States v. Knotts*, denied his motion.[31] The trial court saw no distinction between surveillance conducted using a GPS device and surveillance conducted using a radio beeper because, in both cases, the technology revealed nothing more than what had been knowingly exposed to the public.[32] Although the officers in *Jones* violated the terms of their warrant when installing the GPS device, the trial court found that they were not required to get a warrant in the first place, and therefore, did not violate Jones's Fourth Amendment rights.[33] A jury

24. Gray & Citron, *supra* note 17, at 103.
25. United States v. Jones, 132 S. Ct. 945, 954 (2012).
26. *Id.* at 948.
27. *Id.*
28. *Id.*
29. *Id.*
30. *Id.*
31. United States v. Jones, 451 F. Supp. 2d 71, 88 (D.D.C. 2006), *aff'd in part, rev'd in part sub nom.* United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010).
32. *See id.*
33. *Id.*

subsequently convicted Jones based in part on evidence gathered through the GPS-enabled tracking device.[34]

Jones appealed to the United States Court of Appeals for the District of Columbia Circuit, which reversed.[35] Writing for a unanimous panel, Judge Ginsburg held that *Knotts* did not control.[36] According to Judge Ginsburg, there is a constitutionally significant difference between being tracked and monitored for an afternoon and being tracked and monitored twenty-four hours a day for four weeks.[37] The constitutional line, according to the court of appeals, is marked by reasonable expectations of privacy.[38] We may know and expect that our movements in public will be monitored in snippets and moments by scores of people we see and pass in our daily lives.[39] We may even think it is not unreasonable to expect that some people might, by design or accident, monitor us for slightly longer periods of time.[40] None of us expect, however, that the government, or anyone else, will monitor our movements constantly over an extended period of time.[41] To the contrary, we quite reasonably assume a basic level of anonymity in the aggregate of our public movements.[42] We lead our lives on the assumption that nobody is cataloguing our comings and goings, or assembling informational "mosaics" based on where we go over the course of a week or a month.[43] Accordingly, the District of Columbia Circuit held that law enforcement's use of the GPS-enabled device to track Jones for twenty-eight days was a Fourth Amendment search subject to Fourth Amendment regulation.[44]

On certiorari, the Supreme Court affirmed.[45] Writing for the majority, Justice Scalia declined to articulate any new constitutional principles governing the use of GPS-enabled tracking technologies.[46] He focused instead on traditional principles of physical intrusion and trespass, which have long marked the heartland of Fourth Amendment concerns and regulations.[47] Because the officers physically intruded into a constitutionally protected area (Jones's car was, after all, an "effect") for the purpose of gathering information, Justice Scalia had no reservations in holding that they engaged in a search "within the meaning of the Fourth Amendment when it

---

34. *Jones*, 132 S. Ct. at 948–49.
35. *Maynard*, 615 F.3d at 549.
36. *Id.* at 556–58, 563.
37. *Id.* at 558.
38. *Id.* at 560.
39. *Id.* at 560–63.
40. *See id.* at 560; *see also* Gray & Citron, *Shattered Looking Glass*, *supra* note 21, at 412.
41. *Maynard*, 615 F.3d at 560.
42. *Id.* at 563.
43. *Id.* at 561–63.
44. *Id.* at 563, 568.
45. United States v. Jones, 132 S. Ct. 945, 954 (2012).
46. *Id.*
47. *Id.* at 949–52.

was adopted."[48] Because the officers failed to obey the terms of their warrant, their installation of the device on Jones's car violated his Fourth Amendment rights.[49]

Justice Scalia charted a narrow course in *Jones*. This allowed the Court to rely on well-established constitutional principles governing physical intrusions.[50] In doing so, however, the Court once again declined to elaborate any constitutional principles—be they new or old, different or the same—that might govern the deployment and use of contemporary surveillance technologies.[51] It did, however, spark a broader public conversation by highlighting some of these technologies and exposing to broader public scrutiny the challenges they pose to the security of the people against unreasonable searches.[52]

Most of us can be fairly secure, most of the time, that we are not being tracked by devices like the one used by the officers in *Jones*.[53] That is because it is unlikely that officers will bother with installing or monitoring GPS-enabled trackers without first having some reason to suspect that a target is engaged in criminal activity.[54] Tracking by officer-installed GPS-enabled devices is much more efficient as a means of surveillance than physically tailing a suspect, but it still requires some degree of labor, initiative, and commitment of police resources.[55] We can now take further assurance after *Jones* because government officers' installation of tracking devices on our persons or property is subject to Fourth Amendment restraints.[56] As Justices Sotomayor and Alito pointed out in their concurring

---

48. *Id.* at 949.

49. *Id.* at 954.

50. *Id.* at 949–52.

51. *Id.* at 953–54.

52. *See, e.g.*, Marc Jonathan Blitz, *The Fourth Amendment Future of Public Surveillance: Remote Recording and Other Searches in Public Space*, 63 AM. U. L. REV. 21, 33–38 (2013) (arguing that focusing only on long-term surveillance is an inadequate constitutional protection); Susan Freiwald, *The* Davis *Good Faith Rule and Getting Answers to the Questions* Jones *Left Open*, 14 N.C. J.L. & TECH. 341, 346–51 (2013) (finding the Alito concurrence in *Jones* an incomplete solution); Woodrow Hartzog, *The Fight to Frame Privacy*, 111 MICH. L. REV. 1021, 1040–42 (2013) (concluding that the mosaic theory supports an obscurity-based analysis of privacy); Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 313–14 (2012); Christopher Slobogin, *Making the Most of* United States v. Jones *in a Surveillance Society: A Statutory Implementation of Mosaic Theory*, 8 DUKE J. CONST. L. & PUB. POL'Y 1, 24–25 (2012).

53. *Cf. Jones*, 132 S. Ct. at 948 (using GPS-enabled devices to track individuals suspected of narcotics trafficking).

54. *Cf. id.* at 955 (Sotomayor, J., concurring) (suggesting that the real dangers in GPS-tracking lie not in the use of devices installed by law enforcement but in taking advantage of "factory- or owner-installed vehicle tracking devices or GPS-enabled smartphones").

55. *See id.* at 964–65 (Alito, J., concurring). This may cease to be true given the rapid reduction in costs for these devices. *See supra* text accompanying notes 17–19. But, at any rate, *Jones* reassures against the use of these devices to facilitate programs of broad and indiscriminate surveillance by subjecting the government's installation of tracking devices to Fourth Amendment regulation. *Jones*, 132 S. Ct. at 949 (majority opinion).

56. *Jones*, 132 S. Ct. at 949.

opinions in *Jones*, however, this security is thin to the point of meaninglessness.[57]

Justice Sotomayor joined the majority in *Jones*, but also wrote a separate concurrence.[58] Justice Alito did not join the majority, but instead wrote a concurring opinion in which Justices Ginsburg, Breyer, and Kagan joined.[59] As these five Justices agreed, "physical intrusion is now unnecessary to many forms of surveillance."[60] That is because we routinely carry or travel in the company of GPS-enabled devices, including our smartphones, many "dumb phones," antitheft devices installed in our computers and cars, and "factory- or owner-installed vehicle tracking devices" such as navigation systems and consumer services like OnStar.[61] These devices are all designed to "leak" data regarding where we are and where we have been.[62] Although the primary recipients of this leaked data are the service providers associated with our devices or the operators of various user applications, there is no Fourth Amendment barrier preventing the government from accessing that information from those third parties through lawful means.[63] Thus, law enforcement may need a warrant to install a GPS-enabled tracking device on a suspect or his effects, but they have essentially free access to the same information if they secure it through private third parties, such as our cellular phone providers or application hosts.[64] This provides an opportunity for precisely the kinds of dragnet surveillance programs foreshadowed in *Knotts*.[65] Yet, as Justice Sotomayor points out in *Jones*, we do not yet have constitutional principles capable of addressing, much less limiting, surveillance by these means.[66]

The five concurring Justices in *Jones* could do no more than posit the possibility of broad and indiscriminate government surveillance programs that exploit data shared with private third parties, such as our cellular phone providers.[67] In June 2013, however, their abstract worries became concrete. Documents disclosed by former NSA contractor Edward Snowden revealed surveillance programs including a telephony metadata

---

57. *Id*. at 955 (Sotomayor, J., concurring); *id.* at 962 (Alito, J., concurring).

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

59. *Id*. at 957 (Alito, J., concurring).

60. *Id*. at 955 (Sotomayor, J., concurring); *see also id.* at 961–63 (Alito, J., concurring) (noting the possibility of law enforcement remotely exploiting radio-activated anti-theft devices installed by an auto manufacturer).

61. *Id*. at 955 (Sotomayor, J., concurring).

62. *Id.* at 963 (Alito, J., concurring); *see also* Joshua Fairfield & Christopher Engel, *Privacy as a Public Good*, 62 DUKE L. J. (forthcoming), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2418445 (noting the location-tracking capabilities of modern cell phones).

63. *See Jones*, 132 S. Ct. at 956–57 (Sotomayor, J., concurring) (citing Smith v. Maryland, 442 U.S. 735, 742 (1979) and United States v. Miller, 425 U.S. 435, 443 (1976)).

64. *See id.*

65. *See id.*; *id.* at 962–64 (Alito, J., concurring).

66. *Id.* at 957 (Sotomayor, J., concurring).

67. *See id.* at 955; *id.* at 963 (Alito, J., concurring).

program.[68] As government officials subsequently admitted, the Federal Bureau of Investigation (FBI) and National Security Agency (NSA) have been gathering metadata associated with domestic telephone calls since at least 2001.[69] Starting in 2006, those efforts were consolidated under orders issued by the Foreign Intelligence Surveillance Court (FISC) pursuant to § 215 of the USA PATRIOT Act.[70] Those orders compelled domestic telephone companies to hand over all metadata associated with all domestic telephone calls on a daily basis.[71] That metadata includes telephone numbers of callers and recipients, times and dates of their calls, durations of their calls, and in the past has included routing information, which in turn reveals the locations of call participants.[72] Despite the dragnet nature of this program, most of the courts asked to review its constitutionality have either demurred or found that it does not violate the Fourth Amendment.[73]

As the telephony metadata program shows, GPS technology is not the only game in town when it comes to tracking people through their cellular phones.[74] Both smartphones and their less intelligent forebears communicate constantly with the network of cellular service towers that comprise the infrastructure necessary for wireless communication.[75] Cellular service providers monitor and record these pings, effectively constructing a historical record of cellular phone users' movements over time.[76] Although some state courts have held that government agents should not have free access to this cell site location data under their state constitutions, only one federal court has articulated any Fourth Amendment constraints on the government's ability to access and use this information, even if it is part of a dragnet surveillance program.[77]

---

68. PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT 1 (Jan. 23, 2014), https://www.pclob.gov/library/215-Report_on_the_Telephone_ Records_Program.pdf.

69. *See id.* at 37.

70. *Id.* at 42.

71. *Id.*

72. *Id.* at 21–23 (explaining that telephone companies now remove routing information before handing over call records to the NSA).

73. *See, e.g.*, ACLU v. Clapper, 785 F.3d 787, 824 (2d Cir. 2015) (declining to reach the constitutional questions raised by the § 215 telephony metadata program), *vacating and remanding* 959 F. Supp. 2d 724, 752–54 (S.D.N.Y. 2013) (finding the § 215 telephony metadata program constitutional); Klayman v. Obama, 957 F. Supp. 2d 1 (D.D.C. 2013) (finding the § 215 telephony metadata program unconstitutional on Fourth Amendment grounds), *vacated and remanded*, No.14-5004, 2015 WL 5058403 (D.C. Cir. Aug. 28, 2015).

74. *See* Commonwealth v. Augustine, 4 N.E.3d 846, 853–54 (Mass. 2014) (discussing a cellular service provider's ability to locate a cellular telephone based on the phone's communication with the provider's cell towers).

75. *Id.*

76. *Id.*

77. *See* United States v. Graham, 796 F.3d 332, 338 (4th Cir. 2015), *reh'g en banc granted*, 2015 WL 6531272 (Oct. 28, 2015); *Augustine*, 4 N.E.3d at 853–54 (discussing that for a brief period, law enforcement agencies conducting investigations in the Eleventh Circuit Court of Appeals were required

Some may hope that they are secure from tracking because they do not carry GPS-enabled devices or cellular phones.[78] The contemporary dragnet is much too broad to make this sense of security reasonable, however. For example, security cameras, license plate readers, and other imaging technologies increasingly monitor our public spaces.[79] They are mounted to buildings, utility poles, cars, and sometimes people.[80] These monitoring technologies are transported through the ether on unmanned drones.[81] In isolation, these devices constitute no more of a threat to reasonable expectations of privacy than do persons on the street.[82] Linked together through networks, however, these devices offer governments and law enforcement the opportunity to conduct dragnet visual surveillance on a twenty-four hour basis.[83] Far from science fiction, municipalities such as New York City and states such as Alabama have worked with corporate partners to develop and deploy precisely these sorts of systems, which offer the capacity to conduct both real-time and historical surveillance of anyone moving through public space, whether they have cellular phones or not.[84]

Quite apart from our cellular phones and other GPS-enabled devices, most of us also carry a variety of tracking devices, usually without being aware that they are traceable.[85] Nowadays, there are radio frequency identification device (RFID) tags embedded in passports, many states' drivers' licenses, many credit cards, access cards, and consumer goods ranging from cars to coats.[86] These devices constitute an electromagnetic version of barcodes, communicating embedded information to reader

---

to secure warrants before accessing cell site location information); *see also* United States v. Davis, 754 F.3d 1205, 1212 (11th Cir. 2014), *aff'd en banc*, 785 F.3d 498, 531–32 (11th Cir. 2015) (holding that obtaining records with a warrant was reasonable); *In re* Application of U.S. for Historical Cell Site Data, 724 F.3d 600, 614–15 (5th Cir. 2013) (holding that cell site location information falls within the compass of the third-party doctrine).

78. *See* United States v. Maynard, 615 F.3d 544, 563 (D.C. Cir. 2010) (stating that a reasonable person does not expect anyone is monitoring his movements).

79. Gray & Citron, *supra* note 17, at 63–66.

80. *See* Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 2 (2008).

81. *See* Lev Grossman, *Drone Home*, TIME (Feb. 11, 2013), http://content.time.com/time/magazine/article/0,9171,2135132,00.html; Jennifer Lynch, *Are Drones Watching You?*, ELECTRONIC FRONTIER FOUND. (Jan. 10, 2012), https://www.eff.org/deeplinks/2012/01/drones-are-watching-you. In the United States, "50 companies, universities, and government organizations are developing and producing some 155 unmanned aircraft designs." Lynch, *supra* (quoting a July 15, 2010 FAA Fact Sheet). In 2010, expenditures on unmanned aircrafts in the United States exceeded three billion dollars and are expected to surpass seven billion dollars over the next ten years. *Id.*

82. *See generally* Katz v. United States, 389 U.S. 347, 351 (1967) (holding that individuals lack a reasonable expectation of privacy on information they knowingly expose to the public).

83. Gray & Citron, *supra* note 17, at 65–66.

84. *See id.* at 66–67.

85. *See How to Hide from RFID Chips, Cell Tower Tracking, and Wi-Fi Snoops*, INDEP. LIVING NEWS, http://www.independentlivingnews.com/freebies/free-reports/20617-how-to-hide-from-rfid-chips-cell-tower-tracking-and-wi-fi-snoops.stml (last visited Oct. 14, 2015) (discussing the prevalence of RFID tracking technology and its placement on everyday items including the physical bodies of people).

86. *See* Jonathan Weinberg, *Tracking RFID*, 3 I/S: J.L. & POL'Y INFO. SOC'Y. 777, 779 (2008).

devices.[87] Because RFID tags are unique, and the devices and items to which they are affixed often have unique relationships to users, RFID tags can be and are used to track items, and therefore people, through automatic identification and data capture systems.[88] Most of us have no idea that we are carrying these tags, much less that they increasingly are used to facilitate the kinds of broad and indiscriminate tracking that the Court declined to address in *Knotts* and *Jones*.[89]

As this brief overview of some contemporary tracking technologies shows, the question set aside in *Knotts* is upon us.[90] The government demonstrably engages in "dragnet-type surveillance," and the technology for even broader and more invasive tracking programs is already available and in widening use.[91] Although the Court in *Jones* did not determine what, if any, constitutional principles might guarantee the security of the people against the threats of unreasonable searches posed by these programs, some of the questioning during oral arguments suggests a promising source for those principles: the text and original public meaning of the Fourth Amendment.[92]

III. DIFFERENT CONSTITUTIONAL PRINCIPLES

Chief Justice Roberts offered a hint of some "different constitutional principles" that might govern law enforcement's access to and use of contemporary tracking technologies in a colloquy with Deputy Solicitor General Michael Dreeben during oral argument in *Jones*.[93] As did the Government below, Mr. Dreeben grounded his argument in *Knotts*.[94] According to Mr. Dreeben, Jones had no reasonable expectation of privacy in any of the information gathered by the GPS-enabled tracking device because it gathered only what Jones knowingly exposed to public view.[95] Mr. Dreeben argued that the installation and the use of that device therefore fell outside the scope of Fourth Amendment review and regulation.[96] In

87. *See id.* at 781–84.

88. *See id.* at 783–84, 815–16, 819–21.

89. *See supra* notes 12–16, 46–77 and accompanying text.

90. *See* United States v. Knotts, 460 U.S. 276, 280–84 (1983) (questioning whether monitoring the signal of a suspect's electronic beeper to determine the suspect's whereabouts is a violation of the Fourth Amendment when visually monitoring the suspect's movements on public thoroughfares would reveal the same facts).

91. *Id.* at 283–84; Citron & Gray, *Addressing the Harm*, *supra* note 21, at 265 (explaining the increasing scope of surveillance capacities such as tiny cameras and technologies, which the government and private collaborators utilize to access consumers' online activities and communications).

92. *See generally* United States v. Jones, 132 S. Ct. 945, 949–53 (2012) (explaining the constitutionality of GPS tracking); Transcript of Oral Argument at 5–9, *Jones*, 132 S. Ct. 945 (No. 10-1259), 2011 WL 5360051.

93. *See* Transcript of Oral Argument, *supra* note 92, at 16, 23.

94. *Id*. at 3.

95. *Id.* at 4–5.

96. *Id.*

response, Chief Justice Roberts asked whether it would "be a search if [the government] put a GPS device on all of our cars, [and] monitored our movements for a month."[97] Again relying on *Knotts*, Mr. Dreeben maintained that this would not be a search because "the Justices of this Court when driving on public roadways have no greater expectation of [privacy]."[98]

Based in part on this question, some criticized the Chief Justice, and the Court more broadly, for recognizing the salience of privacy concerns only when their personal privacy is threatened.[99] As this critique goes, the Court is perfectly happy to license some surveillance, such as low-altitude flyovers by helicopters, because the Justices could not imagine themselves being subject to these kinds of searches.[100] By contrast, they could immediately imagine the threat posed by GPS-enabled tracking devices, and therefore imposed Fourth Amendment constraints based purely on selfish motives.[101] There is, however, a much more charitable interpretation of the Chief Justice's question, which also happens to carry significant constitutional weight.[102]

The rights protected by the Fourth Amendment are, first and foremost, collective.[103] This is borne out by the text, which reads, "The right of the people."[104] It is also evident in the historical context in which the Fourth Amendment was written and adopted.[105] The primary targets for the Fourth Amendment were writs of assistance and other forms of general warrants.[106] As then-contemporary commentators pointed out, the primary concern raised by general warrants was the broad license they granted for government agents to conduct searches based solely on their own discretion.[107] Although few

---

97. *Id.* at 9.

98. *Id.* at 9–10.

99. *See, e.g.*, Tamara Rice Lave, *Protecting Elites: An Alternative Take on How* United States v. Jones *Fits into the Court's Technology Jurisprudence*, 14 N.C. J.L. & TECH. 461, 462–65 (2013).

100. *Id.* at 479–80.

101. *Id.* at 484–86.

102. *See infra* notes 103–15 and accompanying text.

103. *See* Gray & Citron, *supra* note 17, at 84–85; *see also* David C. Gray, *Dangerous Dicta*, 72 WASH. & LEE L. REV. (forthcoming 2015), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2601663.

104. U.S. CONST. amend. IV.

105. *See* Gray & Citron, *supra* note 17, at 83–84; Gray, *supra* note 103 (manuscript 5–6).

106. Riley v. California, 134 S. Ct. 2473, 2494 (2014); Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 601 (1999).

107. Osborn v. United States, 385 U.S. 323, 329 n.7 (1966) (stating that the "indiscriminate use of such devices in law enforcement raises grave constitutional questions under the Fourth and Fifth Amendments; and . . . impose a heavier responsibility on this Court in its supervision of the fairness of procedures" (emphasis omitted) (quoting Lopez v. United States, 373 U.S. 427, 441 (1963) (Warren, C.J., concurring))); Johnson v. United States, 333 U.S. 10, 17 (1948) ("An officer gaining access to private living quarters under color of his office and of the law which he personifies must then have some valid basis in law for the intrusion. Any other rule would undermine 'the right of the people to be secure in their persons, houses, papers, and effects,' and would obliterate one of the most fundamental distinctions between our form of government, where officers are under the law, and the police-state where they are the law."); Gray & Citron, *supra* note 17, at 67–73.

colonists were actually victims of searches conducted under the authority of general warrants, their very existence left everyone vulnerable.[108]

Viewed in the light of this history, the Chief Justice's question in *Jones* takes on a different meaning.[109] He viewed the prospect of granting law enforcement unfettered discretion to install and use GPS tracking devices as a threat to the security of every citizen, and therefore, to the security of the people as a whole against unreasonable searches and seizures.[110] If the government could use the devices to track him and his brethren, then they could track anyone and everyone.[111] That very possibility would leave the people insecure in their persons and effects, running afoul of the Fourth Amendment.[112] Traditional constitutional principles, then, bound the Court to limit the discretion of law enforcement to install and use GPS-enabled tracking devices.[113]

Although the *Jones* Court limited the discretion of law enforcement officers to install tracking devices on persons and their effects, it did not limit the use of tracking technologies.[114] The question, therefore, remains whether the constitutional principles alluded to in the Chief Justice's question might also suggest constitutional constraints on the use of native GPS devices, networked surveillance cameras, or RFID tracking.[115] Based on a straightforward reading of the Fourth Amendment in its historical context, the answer, quite clearly, is "yes."

IV. CONSTITUTIONAL CONSTRAINTS ON CONTEMPORARY TRACKING TECHNOLOGIES

The threshold question in any Fourth Amendment analysis is whether the government conduct in question constitutes a search.[116] As the Court pointed out in *Jones*, this inquiry begins by asking whether tracking would have been considered a search by those who wrote and read the Fourth

---

108. Boyd v. United States, 116 U.S. 616, 630 (1886) ("The principles laid down in this opinion affect the very essence of constitutional liberty and security. They reach farther than the concrete form of the case then before the court, with its adventitious circumstances; they apply to all invasions on the part of the government and its employe[e]s of the sanctity of a man's home and the privacies of life."); Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 366 (1974) ("[T]he specific incidents of Anglo-American history that immediately preceded the adoption of the [Fourth A]mendment, we shall find that the primary abuse thought to characterize the general warrants and the writs of assistance was their indiscriminate quality, the license that they gave to search Everyman without particularized cause . . . [which threatened] 'the whole English nation.'" (quoting John Wilkes in *The North Briton* No. 45)).

109. *See* Transcript of Oral Argument, *supra* note 92, at 3–4.

110. *See id.* at 18.

111. *See id.* at 10.

112. *See* United States v. Jones, 132 S. Ct. 945, 954 (2012).

113. *See id.*

114. *Id.*

115. Transcript of Oral Argument, *supra* note 92, at 3–4.

116. *Jones*, 132 S. Ct. at 950 n.3.

Amendment in 1791.[117] According to Samuel Johnson's 1768 Dictionary of the English Language, "to search" meant then what it does now: "[t]o examine," "to explore," "[t]o seek," and "to try to find."[118] By definition, tracking, whether directly or by the use of contemporary and emerging surveillance technologies, constitutes seeking and "trying to find" suspects and other targets.[119] By both eighteenth century and twenty-first century standards, tracking therefore qualifies as a search.[120]

The Fourth Amendment does not prohibit or even purport to regulate all searches and seizures.[121] To the contrary, it only guarantees to the people security against unreasonable searches and seizures.[122] Thus, government tracking can only run afoul of the Fourth Amendment if it threatens the right of the people to be secure from unreasonable searches.[123] As the Court held in *Knotts*, human surveillance, which one might refer to conventionally as "tailing," does not threaten the security of the people against unreasonable searches.[124] The *Knotts* Court also held that the use of a beeper tracking device to assist officers who are tailing a suspect does not threaten the security of the people against unreasonable searches and seizures.[125] The question, then, is whether there is something different about the use of contemporary surveillance technologies that threatens the security of the people against unreasonable searches.

As the *Knotts* Court pointed out, conventional human surveillance, even when augmented by a beeper tracking device, does not raise the specter of "dragnet-type law enforcement practices," such as the "twenty-four hour surveillance of any citizen of [the United States] . . . without judicial knowledge or supervision."[126] That is because human surveillance, even with the assistance of a radio beeper device, is extremely resource-intensive, requiring the dedicated attention of several or even scores of police officers over an extended period of time.[127] As Justice Alito pointed out in his *Jones* concurrence, the effort and cost associated with this type of surveillance means that it is "rarely undertaken," and only in cases of "unusual

---

117. *Id.* at 949–50.

118. *Compare* SAMUEL JOHNSON, DICTIONARY OF THE ENGLISH LANGUAGE (3d ed. 1768), *with* WEBSTER'S NINTH NEW COLLEGIATE DICTIONARY (1985) (defining *search* as "to look into or over carefully or thoroughly in an effort to find or discover something").

119. *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring) (pointing out that the purpose of attaching the GPS-enabled tracking device to Jones's car was to "gather information" about his movements); JOHNSON, *supra* note 118 (defining the verb *track* as "[t]o follow by the footsteps or marks left in the way").

120. *See Jones,* 132 S. Ct. at 949 (majority opinion).

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

122. *Id.*

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

124. United States v. Knotts, 460 U.S. 276, 282 (1983).

125. *Id.* at 282–83, 285.

126. *Id.* at 284 (quoting Brief for Respondent at 9, *Knotts*, 460 U.S. 276 (No. 81-1802)).

127. Gray & Citron, *supra* note 17, at 132.

importance" would a law enforcement agency dedicate the resources necessary to conduct extended surveillance of a suspect.[128] As a consequence, human surveillance, even when conducted with the assistance of radio beepers, simply does not threaten the security of the people against unreasonable searches and seizures because it is not a technology capable of facilitating programs of broad and indiscriminate search.[129]

Government agents are unlikely to deploy the resources necessary to conduct extended human surveillance without good reason.[130] Human surveillance, and particularly extended human surveillance, is therefore unlikely to constitute an unreasonable search.[131] More importantly, however, the resource restraints that limit human surveillance also limit its potential threat to the security of the people from unreasonable searches.[132] Because it is expensive, most of us can be secure that we are not, never have been, and never will be subject to extended human surveillance, whether reasonable or not.[133] This is what the Court meant in *Knotts* when it set aside concerns about "dragnet-type law enforcement practices."[134] It is also the reason why Chief Justice Roberts, speaking on behalf of the people, likely would not be concerned with granting law enforcement an unfettered license to conduct human surveillance of suspects transiting public spaces.[135] Doing so just does not pose a general threat to the security of the people against unreasonable searches.[136]

As Justices Sotomayor and Alito indicated in their *Jones* concurrences, and as Chief Justice Roberts suggested with his question during oral argument in that case, granting government agents unfettered discretion to conduct surveillance using modern tracking technologies does threaten the security of the people against unreasonable searches.[137] That is because these technologies "raise[] the specter of a surveillance state" by enabling "dragnet-type law enforcement practices," including the demonstrated capacity to conduct "twenty-four hour surveillance of any [or every] citizen" for an unlimited period of time.[138] Unlike the beeper technology at issue in *Knotts*, there are no material or resource limits to how many people law enforcement agencies can track using modern technologies, or for how long

---

128. *Jones*, 132 S. Ct. at 945, 963–64 (Alito, J., concurring).

129. *Knotts*, 460 U.S. at 282.

130. *Jones*, 132 S. Ct. at 963–64.

131. *See, e.g.*, United States v. Place, 462 U.S. 696, 703 (1983) (stating that "the Court must balance the nature and quality of the intrusion on the individual's Fourth Amendment interests against the importance of the governmental interests alleged to justify the intrusion").

132. *See Jones*, 132 S. Ct. at 963–64; *see also* Gray & Citron, *supra* note 17, at 132.

133. McAdams, *supra* note 15, at 326.

134. *Knotts*, 460 U.S. at 283–84.

135. *See* McAdams, *supra* note 15, at 326; *supra* notes 97–101 and accompanying text.

136. McAdams, *supra* note 15, at 326.

137. *Jones*, 132 S. Ct. at 955–56 (Sotomayor, J., concurring); *id.* at 964 (Alito, J., concurring); Transcript of Oral Argument, *supra* note 92, at 9–10.

138. *Knotts*, 460 U.S. at 276, 283–84; Gray & Citron, *supra* note 17, at 105–12, 131–33.

the agencies can track people.[139] Granting law enforcement an unlimited license to use these technologies, therefore, leaves each of us and all of us constantly vulnerable to tracking for good reasons, bad reasons, or no reason at all.[140] It is hard to imagine a more direct threat to the security of the people from unreasonable searches.[141]

None of this means that the courts or the legislature should bar law enforcement from using modern tracking technologies.[142] What the Fourth Amendment requires, rather, is some set of prospective restraints on law enforcement's access to and use of these technologies that is sufficient to preserve the security of the people against unreasonable searches conducted using these technologies.[143] As to what form these remedies might take, we can again take instruction from our eighteenth century forebears.

The means and methods that most threatened the security of Americans in 1791 were physical searches of their persons, houses, papers, and effects.[144] Because these searches entailed physical intrusions, the common law of trespass limited the authority of government agents to conduct these sorts of searches.[145] As a result, most persons, and therefore the people, were relatively secure against the threat of unreasonable physical searches.[146] Writs of assistance and other forms of general warrants effectively released government agents from common law restraints, granting them unfettered

---

139. Gray & Citron, *supra* note 17, at 105–12, 131–32.

140. *See id.*

141. *See id*.

142. *See id.* at 107–12.

143. *See* Camara v. Mun. Court of S.F., 387 U.S. 523, 528 (1967) ("The basic purpose of this Amendment, as recognized in countless decisions of this Court, is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials. The Fourth Amendment thus gives concrete expression to a right of the people which 'is basic to a free society.'" (quoting Wolf v. Colorado 338 U.S. 25, 27 (1949))); Weeks v. United States, 232 U.S. 383, 391–92 (1914) ("The effect of the 4th Amendment is to put the courts of the United States and Federal officials, in the exercise of their power and authority, under limitations and restraints as to the exercise of such power and authority, and to forever secure the people, their persons, houses, papers, and effects, against all unreasonable searches and seizures under the guise of law."), *overruled by* Mapp v. Ohio, 367 U.S. 643 (1961). There is no doubt that some current Fourth Amendment remedies, such as the exclusionary rule and § 1983, do less work than they could or ought to in guaranteeing the right of the people to be secure. *See generally* David Gray, *A Spectacular Non Sequitur: The Supreme Court's Contemporary Fourth Amendment Exclusionary Rule Jurisprudence*, 50 AM. CRIM. L. REV. 1 (2013) (explaining the need for the Court to adopt a hybrid approach to the exclusionary rule that acknowledges both the punishment and the principle aspects of the rule); David Gray, Meagan Cooper & David McAloon, *The Supreme Court's Contemporary Silver Platter Doctrine*, 91 TEX. L. REV. 7 (2012) (explaining that the Court's adoption of the collateral use exception to the exclusionary rule constitutes a move back towards the silver plate doctrine, which allowed the use of evidence from unreasonable searches and seizures); Jennifer E. Laurin, *Trawling for* Herring*: Lessons in Doctrinal Borrowing and Convergence*, 111 COLUM. L. REV. 670 (2011) (discussing the consequences of the Court's decision in *Herring v. United States*, 555 U.S. 135 (2009), and whether borrowing and convergence ideals help explain changes in the exclusionary rule).

144. Gray, *supra* note 23; Gray, *supra* note 103.

145. Olmstead v. United States, 277 U.S. 438, 465 (1928), *overruled in part by* Katz v. United States, 389 U.S. 347 (1967); Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 786 (1994).

146. *See* Amar, *supra* note 145.

discretion to search anyone, anywhere, anytime, and for any reason or no reason.[147] As contemporary critics pointed out, the very existence of general warrants therefore threatened the security of the people against unreasonable searches.[148]

Faced with the general threat to security posed by writs of assistance, our founders settled on a simple solution: the Warrant Clause.[149] By prohibiting general warrants and setting limits on when, in what circumstances, and by whom specific warrants could issue, the warrant clause restored the security of the people against unreasonable physical searches licensed by general warrants.[150] They knew that government agents who proceeded without warrants would be subject to the threat of civil action, and therefore would be less likely to engage in unreasonable searches.[151] They also knew that government agents who conducted searches licensed by a warrant would need to meet the stringent demands of showing probable cause and particularity before a detached and neutral magistrate, making the possibility of unreasonable warranted searches far less likely.[152]

Through the combination of *ex ante* restraint and the threat of *ex post* discipline, the Warrant Clause was able to guarantee the security of the people against unreasonable physical searches of their persons, houses, papers, or effects.[153] The absence of any Fourth Amendment cases of any consequence between 1791, when the Fourth Amendment was ratified, and 1886, when *Boyd v. United States* ushered in an era during which the Court struggled to rein in new threats posed by the rise of professionalized, paramilitary police departments, is evidence of the Warrant Clause's success in this endeavor.[154] Threats of civil action proved insufficient to constrain these new institutions and their zealous agents.[155] In response, the Court instituted the warrant requirement, which restored the security of the people

147. *See id.* at 767, 774; VA. CONST. art. I, § 10 (West, Westlaw through End of the 2015 Reg. Sess.) (defining *general warrants* as warrants "whereby any officer or messenger may be commanded to search suspected places without evidence of a fact committed, or to seize any person or persons not named, or whose offense is not particularly described and supported by evidence"); *see also* United States v. Poller, 43 F.2d 911, 914 (2d Cir. 1930) ("[T]he real evil aimed at by the Fourth Amendment is the search itself, that invasion of a man's privacy which consists in rummaging about among his effects to secure evidence against him.").

148. *See* Amar, *supra* note 145, at 776–77. In his famous argument in the writs of assistance cases, James Otis identified general warrants as "the worst instrument of arbitrary power, the most destructive of English liberty and the fundamental principles of law, that ever was found in an English law book." Boyd v. United States, 116 U.S. 616, 625 (1886) (quoting James Otis (1761)); *see also* Silas J. Wasserstrom, *The Fourth Amendment's Two Clauses*, 26 AM. CRIM. L. REV. 1389, 1393 (1989) (stating that the founders "sought to prohibit the newly formed federal government from using general warrants, a device they believed jeopardized the liberty of every citizen").

149. Gray, *supra* note 23.

150. *Id.*

151. *Id.*

152. *Id.*

153. *Id.*

154. *Id.*

155. *Id.*

against unreasonable searches by interposing courts between law enforcement agents and citizens.[156]

Modern tracking technology may be unprecedented in terms of its capacity to enable programs of broad and indiscriminate searches.[157] These technologies do not, however, tax the conceptual resources of the Fourth Amendment as a guarantor of the people's security against unreasonable searches.[158] As was the case in 1791, and again in the late eighteenth and early nineteenth centuries, the principal challenge is to understand the threats posed by these technologies, and then to set prospective constraints on governments' access to, and use of, these technologies such that the security of the people from unreasonable searches can be restored and maintained.[159]

As it was a hundred years ago, a warrant requirement seems like the most effective, enforceable, and parsimonious means for achieving this goal with respect to discrete surveillance technologies used for tracking purposes.[160] There can be little doubt that most people would be secure that they were not being tracked most of the time if the courts required law enforcement agents to secure a warrant before using technologies like GPS or RFID to track people.[161] Given courts' and law enforcement's long experience with the warrant requirement for physical searches of constitutionally protected areas, there are also good grounds for believing that a warrant requirement for modern tracking technologies would be relatively easy to enforce.[162] Finally, a warrant requirement would strike a parsimonious balance between legitimate law enforcement interests and the right of the people to be secure against unreasonable searches.[163] Tracking technologies are most likely to serve legitimate government needs in the context of active investigations in which agents have identified particular suspects.[164] By contrast, the threats posed by these technologies are most present when law enforcement deploys them in support of "dragnet-type law enforcement practices."[165] By allowing law enforcement access to modern tracking technologies when they have a demonstrated specific interest in an individual based on probable cause, but barring the broad, indiscriminate, or purely discretionary use of these technologies, a warrant requirement would strike an appropriate and reasonable balance between competing interests in law enforcement and privacy.[166]

---

156. *Id.*
157. *See supra* Part II.
158. *See supra* notes 114–15 and accompanying text.
159. *See supra* notes 142–56 and accompanying text.
160. Gray & Citron, *supra* note 17, at 104–05.
161. *See supra* notes 139–40 and accompanying text.
162. *See supra* notes 149–52 and accompanying text.
163. *See* Gray & Citron, *supra* note 17, at 111–12.
164. *See id.*
165. *Id.* at 105; United States v. Knotts, 460 U.S. 276, 284 (1983).
166. Gray & Citron, *supra* note 17, at 107–08.

V. CONCLUSION

Although brief, this Article provides good grounds for the conclusion that tracking citizens using contemporary surveillance technologies constitutes a search.[167] Furthermore, this Article has shown why granting government agents unfettered discretion to deploy and use these technologies would threaten the security of the people against unreasonable searches in precisely the same way that general warrants threatened the security of the people against unreasonable searches in 1791.[168] Finally, it has suggested one way to restore the security of the people against unreasonable searches conducted using modern tracking technologies without unreasonably compromising legitimate law enforcement goals: a warrant requirement.[169]

167. *See supra* notes 109–13 and accompanying text.
168. *See supra* notes 137–49 and accompanying text.
169. *See supra* notes 160–66 and accompanying text.