

PRIVACY IN THE AGE OF SMARTPHONES: A Better Standard for GPS Tracking

Andrew McNichol*

INTRODUCTION

Imagine a scenario in which you are going about your daily business. You visit a friend, grab lunch, have a doctor's appointment, go grocery shopping, and then go home and get ready for a night out on the town. Throughout your day, you did not have any encounters with, or even see, a police officer. Surely there's no way the police knew where you were. Surely they couldn't be tracking and recording your movements. However if you, like many people, brought your smartphone with you to all of these activities, police may have an accurate log of your daily travels. Virtually all modern smartphones are equipped with a GPS device capable of tracking a user's location within twenty-five feet.¹ The smartphone owner can use this feature to help locate a new coffee shop or to correct a wrong turn.² But because of the way a smartphone works, this GPS data is necessarily transmitted to the cell carrier as well.³

This comment argues that society recognizes an individual's expectation of privacy in the GPS data emitted by his smartphone as reasonable, and consequently the use of such data by law enforcement officers constitutes a search within the meaning of the Fourth Amendment that is subject to the warrant requirement.

Part I of this comment details the history of the Supreme Court's Fourth Amendment cases related to GPS devices and tracking. Part II analyzes the treatment of GPS tracking devices in smartphones under the Supreme Court's case law, and exposes the flaws with the current methodology. Part III proposes a better standard to use for analyzing GPS tracking by police:

*. Managing Editor, Arizona State Law Journal; J.D. Candidate, May 2013, Sandra Day O'Connor College of Law at Arizona State University. Thank you Professor Carissa Hessick for your advice and support while researching and writing this note. The author hopes that this note serves as a warning, and not as an instruction manual, for future government tracking of smartphones.

1. See *infra* notes 8–9 and accompanying text.

2. See Eric A. Taub, *When an Android Phone Becomes a GPS Device*, N.Y. TIMES, Aug. 17, 2011, <http://travel.nytimes.com/2011/08/18/technology/personaltech/when-an-android-phone-becomes-a-gps-device.html?pagewanted=all>.

3. See *infra* notes 10–11 and accompanying text.

whether an individual, as well as society, recognizes a reasonable expectation of privacy in an individual's smartphone.

I. THE HISTORY OF GOVERNMENTAL LOCATION TRACKING

A. *How GPS Devices and Smartphones Operate*

Police use GPS technology to track property other than vehicles. More specifically, police may track an individual's location through his smartphone.⁴ The smartphone—a term meaning smartphones that include many of the features of a personal computer⁵—has become a necessity in everyday life. Such devices, capable of accessing email, calendars, and the internet virtually everywhere, recently surpassed fifty percent market share of all smartphones in the United States,⁶ and that number will only increase. One prediction estimates that over five billion individuals worldwide will have smartphones within the next five years.⁷

While smartphones are becoming increasingly common, their capabilities are also increasing. Nearly all smartphones manufactured today include a built-in GPS device.⁸ Such a device is capable of determining and tracking the user's location in real-time, and is accurate to within twenty-five feet.⁹ If you were to track a person's location through their GPS devices, you could likely tell which room in a house or building they were in, but could probably not tell exactly where they were within the room.

But the very nature of the smartphone's GPS device makes its location known to others besides the user. In order to transmit calls and data, a smartphone must communicate with nearby cell towers.¹⁰ This process is

4. See Declan McCullagh, *Justice Dept. to Defend Warrantless Cell Phone Tracking*, CNET (Oct. 2, 2012, 4:00 AM), http://news.cnet.com/8301-13578_3-57524109-38/justice-dept-to-defend-warrantless-cell-phone-tracking/.

5. *Definition of Smartphone*, MERRIAM-WEBSTER.COM, <http://www.merriam-webster.com/dictionary/smartphone> (last visited Oct. 27, 2013).

6. See *America's New Mobile Majority: A Look at Smartphone Owners in the U.S.*, NIELSEN NEWSWIRE (May 7, 2012), http://blog.nielsen.com/nielsenwire/online_mobile/who-owns-smartphones-in-the-us/.

7. See John D. Sutter, *How Smartphones Make Us Superhuman*, CNN.COM (Sept. 10, 2012, 12:16 PM), <http://www.cnn.com/2012/09/10/tech/mobile/our-mobile-society-intro-oms/index.html>.

8. See generally Adam Cohen, *What Your Cell Phone Could Be Telling the Government*, TIME.COM (Sept. 15, 2010), <http://www.time.com/time/nation/article/0,8599,2019239,00.html>.

9. See *GPS Accuracy*, GPS.GOV, <http://www.gps.gov/systems/gps/performance/accuracy/> (last updated Sept. 18, 2013).

10. See generally *In re Application of U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel.*, 460 F. Supp. 2d 448, 450–51 (S.D.N.Y. 2006).

initiated when the user places a call, sends a text message, or accesses the internet through his smartphone. It can also be initiated by third parties: whenever someone calls or sends a text message to a smartphone, the cell towers must locate the smartphone in order to transmit the call or data to it. Commonly referred to as “pinging,” this process forces the smartphone to transmit its location data to the nearby cell towers.¹¹ Pinging is a passive process; it gives no indication to the user that the phone is communicating with a nearby cell tower.¹²

Law enforcement officers are also capable of passively pinging an individual’s smartphone. Dialing the phone number assigned to that particular phone and quickly hanging up will passively ping the phone.¹³ The phone will not ring, but it will transmit its location to a nearby cell tower.¹⁴ By engaging in this process, officers can create a trail of “bread crumbs” that will reveal both historic and real-time location data for smartphones. Every time the phone pings a nearby cell tower, data from the phone is transmitted to the service provider, including the phone’s GPS location. This data is recorded and stored by the service provider.¹⁵

Ordinarily, law enforcement officials need a warrant supported by probable cause in order to obtain an individual’s private records.¹⁶ But 18 U.S.C. § 2703(d) allows a judge to issue an order compelling disclosure of telephone records, which include both historic and real-time location data, as well as a log of calls dialed and received from the phone, as long as there are “reasonable grounds to believe that the contents . . . are relevant and material to an ongoing investigation.”¹⁷ In its application for a § 2703(d) order, the government need only show “specific and articulable facts” rather than the higher probable cause standard.¹⁸

The substance of § 2703 was enacted in 1996, well before smartphones existed.¹⁹ While GPS devices became available for civilian use in 1995, they were not incorporated into phones until much later.²⁰ It is clear then, that § 2703 was not meant to deal with a person’s location data, but rather

11. See *United States v. Skinner*, 690 F.3d 772, 775–76 (6th Cir. 2012).

12. See *id.* at 774.

13. *Id.* at 778.

14. *Id.*

15. *Id.* at 776.

16. See Comment, *Third Circuit Allows Government to Acquire Cell Phone Tracking Data*, 124 HARV. L. REV. 1580, 1584 (2011).

17. Stored Communications Act, 18 U.S.C. § 2703(d) (2010).

18. See Orin S. Kerr, *A User’s Guide to the Stored Communications Act, and a Legislator’s Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1219 (2004).

19. Act of Oct. 11, 1996, Pub. L. 104-294, Title VI, § 605(f), 110 Stat. 3510 (1996).

20. See *Frequently Asked Questions*, GPS.GOV, <http://www.gps.gov/support/faq/> (last updated Sept. 9, 2013).

his historical telephone records. These records would be restricted to only the numbers that a person had previously called.

The practice of police tracking GPS location data has become so common that Verizon Wireless, AT&T, Sprint, and T-Mobile have each created websites accessible by law enforcement agencies specifically for data requests.²¹ These disclosures do not come free; the above listed wireless service providers charge law enforcement agencies high access rates for such information.²² In 2011, AT&T generated revenue of \$8.3 million from these fees alone.²³ In order to handle the increasing number of requests, these companies “employ[] large teams of in-house lawyers, data technicians, phone ‘cloning specialists’ and others around the clock to take requests from law enforcement agencies, review the legality and provide the data.”²⁴ As this practice has grown so substantially over recent years, courts should reexamine their doctrine regarding the privacy of such information.

B. *The Supreme Court’s Treatment of GPS Devices and Their Predecessors*

The Fourth Amendment guarantees the right of the people to be free from “unreasonable searches and seizures.”²⁵ However, defining a search or seizure is not always a simple task.²⁶ Moreover, there are government actions that amount to a search or seizure, yet are still permissible.²⁷ Exigent circumstances, such as public safety concerns, can override an individual’s privacy interest and permit a search or seizure that would otherwise be unreasonable.²⁸ The scope of an individual’s Fourth Amendment right also varies based on his location: an individual in his home is afforded more protection than that same individual when traveling in public.²⁹ A person

21. See Andy Greenberg, *These Are the Prices AT&T, Verizon and Sprint Charge for Cellphone Wiretaps*, FORBES (Apr. 3, 2012, 3:01 PM), <http://www.forbes.com/sites/andygreenberg/2012/04/03/these-are-the-prices-att-verizon-and-sprint-charge-for-cellphone-wiretaps/>.

22. *Id.*

23. Eric Lichtblau, *Wireless Firms are Flooded by Requests to Aid Surveillance*, N.Y. TIMES, July 8, 2012, <http://www.nytimes.com/2012/07/09/us/cell-carriers-see-uptick-in-requests-to-aid-surveillance.html?pagewanted=all>.

24. *Id.*

25. U.S. CONST. amend. IV.

26. See, e.g., *Terry v. Ohio*, 392 U.S. 1, 8–9 (1968).

27. See, e.g., *United States v. Santana*, 427 U.S. 38, 38–39 (1976).

28. See, e.g., *New York v. Quarles*, 467 U.S. 649, 655–56 (1984); *Terry*, 392 U.S. at 27.

29. See *Payton v. New York*, 445 U.S. 573, 573–74 (1980).

who is at a house solely for business reasons is also given less protection than a person using a home for residential purposes.³⁰

Justice Harlan's concurring opinion in *Katz v. United States*³¹ created the two-pronged test to determine when a government action constitutes a search within the meaning of the Fourth Amendment. First, an individual must exhibit a subjective privacy interest in his property or information; he must take steps to shield personal property or information from the public eye.³² Second, society must recognize the individual's expectation of privacy as reasonable.³³ When a government action violates the reasonable expectations of both the individual and society, it amounts to a search under the Fourth Amendment. Conversely, if society does not recognize an expectation of privacy as reasonable, a government action that infringes on that privacy expectation is not a search under the Fourth Amendment, regardless of an individual's personal expectations.

The Supreme Court first applied the *Katz* two-pronged analysis to tracking devices in *United States v. Knotts*.³⁴ There, police officers installed a beeper³⁵ in a five-gallon container of chloroform with the consent of the owner.³⁶ The owner then sold the container to a codefendant of Knotts, who had no knowledge of the beeper.³⁷ Officers used the beeper to track the defendant's travel on the highway, and subsequently to the defendant's cabin.³⁸ Officers used this information to obtain and execute a warrant of the cabin, where they discovered a drug laboratory.³⁹ The defendant moved to suppress evidence derived from the use of the beeper, arguing that the police violated his Fourth Amendment reasonable expectation of privacy by monitoring his location through the beeper.⁴⁰

The Court held that the use and monitoring of the beeper did not violate the defendant's Fourth Amendment expectations of privacy, as the defendant, by traveling on public highways, voluntarily conveyed his location to the public.⁴¹ An individual has no reasonable expectation of

30. *Minnesota v. Carter*, 525 U.S. 83, 89–90 (1998).

31. 389 U.S. 347 (1967) (Harlan, J., concurring).

32. *Id.* at 361 (Harlan, J., concurring).

33. *Id.*

34. 460 U.S. 276 (1983).

35. A beeper is the predecessor to the modern day GPS device. Although it does not possess all of the same capabilities as a GPS device, the differences for purposes of this comment are immaterial.

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

37. *Id.*

38. *Id.* at 278–79.

39. *Id.* at 279.

40. *Id.*

41. *Id.* at 281.

privacy in information voluntarily conveyed to a third party, whether it is a phone number or bank records.⁴² The Court treated an individual's location the same way: by voluntarily conveying information to the public, an individual no longer has any subjective expectation of privacy in that information.⁴³ Consequently, the Court concluded that police tracking of the defendant's location through the beeper did not amount to a search within the meaning of the Fourth Amendment.⁴⁴

The Supreme Court again addressed the location tracking issue in *United States v. Karo*.⁴⁵ In *Karo*, a beeper was installed into a can of ether with the consent of the can's owner.⁴⁶ The can was then sold to one of Karo's codefendants, who had no knowledge of the beeper.⁴⁷ Police officers used the beeper to track the can's location on public roads and in Karo's private residence.⁴⁸ Relying on the information obtained from the beeper, officers obtained and executed a search warrant of the defendant's residence, where they discovered an illegal drug operation.⁴⁹ The Court held that monitoring of the beeper while it was on public highways was permissible, as the defendant voluntarily conveyed his location.⁵⁰ However, the monitoring of the beeper while it was in the defendant's residence was a search within the meaning of the Fourth Amendment, as the defendant had a reasonable expectation of privacy in his home.⁵¹

Twenty-eight years later, the Court again addressed the constitutionality of the tracking of a suspect's location. In *United States v. Jones*,⁵² police officers suspected an individual of selling narcotics.⁵³ The government obtained a warrant for the installation of a GPS tracking device onto the bottom of the suspect's car.⁵⁴ Agents then installed a small GPS device onto

42. See *Smith v. Maryland*, 442 U.S. 735, 744 (1979) (finding no reasonable expectation of privacy in a phone number dialed, because that information is also disclosed to a third party phone company); *United States v. Miller*, 425 U.S. 435, 442–43 (1976) (finding no reasonable expectation of privacy in bank records, because federal law requires a bank to maintain and make available certain financial documents).

43. *Knotts*, 460 U.S. at 281–82.

44. *Id.* at 285.

45. 468 U.S. 705 (1984).

46. *Id.* at 708–09.

47. *Id.*

48. *Id.*

49. *Id.* at 710.

50. *Id.* at 721.

51. *Id.*

52. 132 S. Ct. 945 (2012).

53. *Id.* at 948.

54. *Id.*

the suspect's car, but not in the manner authorized by the warrant.⁵⁵ The agents used this device to monitor the suspect's movements.⁵⁶ The government conceded that it did not comply with the warrant, but argued that no warrant was needed for this action.⁵⁷

The Supreme Court held that the secret installation of a GPS device onto the bottom of the defendant's car by police officers without a warrant was a trespass, and amounted to a search within the meaning of the Fourth Amendment.⁵⁸ By deciding the case on the threshold question of constitutionality of the *installation* of the GPS device, the Court did not decide whether the *monitoring* of the GPS device was a search.⁵⁹ As this search was conducted without a warrant or other exigent circumstance, it was unreasonable.⁶⁰ *Jones* differs from both *Knotts* and *Karo*, as the monitoring device in *Jones* was installed on the defendant's property while he owned it, whereas the installation of the monitoring devices in *Knotts* and *Karo* occurred prior to the defendants coming into possession or ownership of the property.⁶¹ The prior owners of the property in *Knotts* and *Karo* consented to the installation of the device; *Jones* obviously did not give any such consent.⁶²

The Court specifically declined to determine whether there had been an invasion of the defendant's privacy interests that amounted to a search.⁶³ Rather, the Court reasoned that the "*Katz* reasonable-expectation-of-privacy test has been *added* to, but not *substituted for*, the common-law trespassory test."⁶⁴ Government actions that are common-law trespass, like *Jones*, are a search within the meaning of the Fourth Amendment. But an individual's Fourth Amendment protections against unreasonable searches do not end there. A government action that is not a common-law trespass is still subject to the *Katz* two-pronged analysis.⁶⁵

While concurring in the result, Justice Alito, joined by Justices Ginsburg, Breyer, and Kagan, attacked the majority's opinion for deciding the case

55. *Id.* The agents installed the GPS device after eleven days, rather than within the ten-day timeframe the warrant authorized. *Id.* The warrant also authorized the agents to install the device on the car within the District of Columbia, but the agents installed the device while the car was parked in Maryland. *Id.*

56. *Id.*

57. *Id.* at 948 n.1.

58. *Id.* at 954.

59. *Id.*

60. *Id.* at 949.

61. *Id.*

62. *Id.*

63. *Id.* at 953–54.

64. *Id.* at 952.

65. *Id.* at 953.

“based on 18th-century tort law.”⁶⁶ Justice Alito “would analyze the question presented in this case by asking whether respondent’s reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle he drove.”⁶⁷ Under this view, the distinction between a GPS tracking device, and police physically following a suspect would disappear.⁶⁸ The monitoring of a suspect through either method would be analyzed under the same question: whether police officers violated the individual’s reasonable expectations of privacy.⁶⁹ Short-term tracking of a suspect, whether through GPS or physical surveillance, would be permissible, while long-term tracking under either method would not.⁷⁰

C. *A Lesser Standard Than Probable Cause Is Being Used*

In *United States v. Skinner*,⁷¹ police obtained an order under 18 U.S.C. § 2703(d) authorizing the phone service company to release the defendant’s cell records, which included historic and real-time location data.⁷² The defendant challenged his conviction, arguing that police infringed on his Fourth Amendment rights by obtaining this information without a search warrant.⁷³ The Sixth Circuit affirmed Skinner’s conviction, holding that there was no Fourth Amendment violation. The court reasoned that the defendant had no legitimate expectation of privacy in his location while traveling on a public highway.⁷⁴ As Skinner did not have any expectation of privacy in his physical location, he also “did not have a reasonable expectation of privacy in the [location] data given off by his voluntarily procured . . . cell phone.”⁷⁵ The court then found that “[t]here is no inherent constitutional difference between trailing a defendant and tracking him via such technology.”⁷⁶ Police monitoring of the defendant’s location was not a search within the meaning of the Fourth Amendment, because Skinner did not have any reasonable expectation of privacy. The court also cited public policy reasons for its decision, stating that it would be unfair to prevent law

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

67. *Id.* at 958.

68. *Id.* at 961.

69. *See id.*

70. *Id.*

71. 690 F.3d 772 (6th Cir. 2012).

72. *See id.* at 776.

73. *Id.* at 777.

74. *Id.* at 779.

75. *Id.* at 777.

76. *Id.* at 778.

enforcement agencies from taking advantage of new technologies while suspects are permitted to gain the benefits of such technology.⁷⁷

The *Skinner* court is the first, and to date the only, circuit court to address this specific issue: whether police location tracking of a suspect's smartphone under §2703 violates the Fourth Amendment's prohibition against unreasonable searches and seizures. Given the court's blessing of the police conduct, it is likely that other state and federal law enforcement agencies will follow suit. As this issue reaches other circuits, they may decide that this practice violates the Fourth Amendment. If the Supreme Court had decided *Jones* on the basis of privacy rather than trespass, it could have prevented a likely circuit split. It seems highly likely that the Court will have to address this issue in an upcoming term.

II. PROBLEMS IN THE CURRENT METHODOLOGY: PHYSICAL TRESPASS IS NOT THE PROPER STANDARD

The current approach that courts use to analyze the constitutionality of electronic location tracking by police officers has several major flaws. First, the analysis focuses too much on physical trespass. Second, the approach ignores the *Katz* two-pronged test. The approach does not examine whether society views an individual's expectation of privacy in his aggregate movements to be reasonable. Additionally, Justice Alito's suggested approach in *Jones* suffers from a major flaw: it permits different levels of tracking based on the crime being investigated. This approach finds no support in any Supreme Court precedent.

The Supreme Court reached the correct result in *Jones*, but it decided the issue on too narrow of a basis. Rather than examining an individual's expectation of privacy as related to electronic tracking by police officers, the Court only decided the issue in the context of trespass. While the Court contemplated "some future case where a classic trespassory search is not involved," it declined to address the hypothetical issue.⁷⁸ However, the Court mischaracterized the case in front of it. *Jones* presented a situation where the Court could have decided these important questions, rather than resolve the case on the trespass issue.⁷⁹ Addressing privacy concerns would

77. *Id.* at 777.

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

79. *See generally* Sherry F. Colb, *The Supreme Court Decides the GPS Case*, *United States v. Jones, and the Fourth Amendment Evolves*, JUSTIA.COM (Feb. 15, 2012), <http://verdict.justia.com/2012/02/15/the-supreme-court-decides-the-gps-case-united-states-v-jones-and-the-fourth-amendment-evolves-2> (stating that the Court focused solely on *when* the police placed the tracking device on the vehicle to distinguish this case from *Knotts*).

provide clear guidance for courts to follow.⁸⁰ Without clear guidance from the Supreme Court, lower courts will split on the issue of police GPS tracking without an accompanying physical trespass.⁸¹

After *Jones*, police officers face many uncertainties regarding the use of GPS tracking devices. What is clear is that officers may not engage in a physical trespass against a suspect's property in order to electronically track the suspect's movements. But there are now technologies available to police officers that allow them to track a suspect's movements without any physical trespass.⁸²

It remains unclear whether these methods are constitutional after *Jones*. While *Karo* and *Knotts* give some guidance to law enforcement officials and restrict location tracking inside a suspect's home, they do not sufficiently cover new and emerging technologies. Additionally, *Jones* focused on when the GPS device was installed. Prior Supreme Court cases held that the installation of a tracking device on a piece of property prior to the defendant coming into possession of that property was *not* a trespass.⁸³ In these cases the Court suggested a *caveat emptor* approach—the purchaser takes property as it comes, tracking device and all.⁸⁴

Justice Alito's approach in *Jones*, although not focusing on the physical trespass, still has many flaws.⁸⁵ Alito suggests an approach that “ask[s] whether the use of GPS tracking in a particular case involved a degree of intrusion that a reasonable person would not have anticipated.”⁸⁶ If the Court adopted Alito's approach, the right of the police to track an individual's movements would depend on both the crime being investigated and the length of the surveillance. This would result in an odd situation: the constitutionality of police actions would depend on the crime being investigated.⁸⁷ The practical problem of determining the appropriate surveillance time limits allowed for various crimes aside, there is a more

80. See *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring) (contemplating a situation where government officials track a smartphone's GPS device without a physical trespass).

81. See *Skinner*, 690 F.3d at 780 (holding that there is no Fourth Amendment violation in tracking a cell phone's location without a physical trespass); *United States v. Barajas*, 710 F.3d 1102, 1108 (10th Cir. 2013) (assuming, without deciding, that cell phone pinging is a search); *United States v. Anderson-Bagshaw*, 509 F. App'x 396, 419 (6th Cir. 2012) (finding that video-surveillance of defendant, even without a physical trespass, was a Fourth Amendment violation).

82. See *United States v. Skinner*, 690 F.3d 772, 778 (6th Cir. 2012).

83. See *supra* notes 34–51 and accompanying text.

84. *United States v. Knotts*, 460 U.S. 276, 286 (1983) (Brennan, J., concurring).

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

86. *Id.*

87. See *id.* at 954 (questioning whether a six-month tracking period would be a permissible for a suspected terrorist, but not for a suspected drug trafficker).

fundamental problem with this approach. Constitutional rights are rights afforded to all individuals—both those suspected of crimes and those who are not. A Fourth Amendment violation is no less a violation because it targeted a particular crime or suspect; all searches involve potential suspects. While exceptions to the Fourth Amendment exist, these involve exigent circumstances that require spur of the moment decisions,⁸⁸ rather than the long and calculated nature posed by location tracking.

Smartphones present a unique scenario. They come pre-installed with a GPS device and emit signals that do not require police to physically trespass to in order to determine their locations. Unlike in *Jones*, smartphones do not require police to install any device onto the phone in order to track its location. The privacy expectations of a smartphone user therefore cannot turn on whether a physical trespass has occurred, because police tracking of a smartphone will never involve a physical trespass. Traditionally “[t]respass to chattels has traditionally required a physical touching of the property.”⁸⁹ Courts have struggled with the concept of trespass in the context of wireless signals, as a signal can touch others’ property, but not in a traditional physical sense.⁹⁰ The limited instances where courts have held an electronic signal to be a trespass to chattels involve signals that interfere in some meaningful way with the chattel: usually a signal that disrupts the use of some other electronic device.⁹¹ Police tracking of a wireless signal presents a different situation, as it does not interfere with the use of the smartphone. Police do not need to install any tracking device on the smartphone. If the installation of a tracking device by police was required, the installation would likely be noticed by the suspect and would thwart police efforts.

The Sixth Circuit’s decision in *Skinner* also does not provide the correct analysis of the constitutionality of police location tracking. The court states that “[i]f a tool used to transport contraband gives off a signal that can be tracked for location, certainly the police can track the signal.”⁹² There are

88. See *Kentucky v. King*, 131 S. Ct. 1849, 1853–54 (2011) (holding that a warrantless entry and search into a home was permissible when there was reason to believe that the inhabitants were destroying evidence); *supra* notes 27–28 and accompanying text.

89. *Jones*, 132 S. Ct. at 962 (questioning under what circumstances a wireless signal could be a trespass to chattels).

90. See *United States v. Karo*, 468 U.S. 705, 712–13 (1984).

91. See, e.g., *CompuServe, Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015, 1021 (S.D. Ohio 1997) (holding that an unwanted wireless signal that interfered with the use of a computer system was a trespass to chattels); *Thrifty-Tel, Inc. v. Bezenek*, 54 Cal. Rptr. 2d 468, 472–73 (Cal. Ct. App. 1996) (same); *State v. McGraw*, 480 N.E.2d 552, 553–54 (Ind. 1985) (use of state’s computer by defendant for more than authorized functions was conversion).

92. *United States v. Skinner*, 690 F.3d 772, 777 (6th Cir. 2012).

two major flaws with this conclusion. First, this reasoning implicitly assumes that because the smartphone was used in the transportation of contraband, the defendant has no reasonable expectation of privacy in it. The privacy interest in a smartphone, or any property,⁹³ exists without consideration of the use of that property. As a smartphone itself is not contraband, the same expectations of privacy exist for both the innocent smartphone user and the drug kingpin who uses a smartphone to facilitate his trade.⁹⁴ Holding otherwise would erode the expectations of privacy for both the innocent and the guilty. It is far from clear which individuals are involved in illegal activities. Allowing the police to track the smartphone of individuals suspected of engaging in such activities ignores the Fourth Amendment's protection against unreasonable searches.

The second problem with this reasoning is its implication that because a device emits a signal, that signal must be obtainable by police. The *Skinner* Court compares a smartphone's trackability to the ability of police dogs to follow the scent of a suspect and to the ability of officers to follow a car based on its license plate, and it argues that, because both of these methods allow officers to track a suspect's location without a warrant, a smartphone's GPS location must also be trackable without a warrant.⁹⁵ Both of these analogies fall short. Under the *Katz* two-pronged test, both the individual and society must recognize a legitimate expectation of privacy in order to have a privacy interest.⁹⁶ A license plate's purpose is to broadcast its numbers and letters to the public. There can be no expectation of privacy, either by society or by an individual, in information voluntarily disclosed to the general public.⁹⁷ Similarly, a suspect traveling in public necessarily leaves his scent available for tracking just as much as he leaves his footprint available for tracking. That the human olfactory sense cannot

93. Any property means any property that is not itself contraband. The Supreme Court has stated that there can be no privacy interest in contraband. *United States v. Jacobson*, 466 U.S. 109, 121 (1984). However, a cell phone is not contraband, even if it is used by those trafficking in contraband. *See Skinner*, 690 F.3d at 785 (Donald, J., concurring) ("Skinner's phone was not contraband and his possession of the phone was not illegal.").

94. *See, e.g., United States v. Pitts*, 322 F.3d 449, 458 (7th Cir. 2003) (finding that a person retains a privacy interest in a cell phone, even if he uses it to facilitate an illegal drug trade); *United States v. Fields*, 113 F.3d 313, 321 (2d Cir. 1997) (finding that privacy expectations in an apartment are the same, whether it is used for criminal or innocent activities); *United States v. Taborda*, 635 F.2d 131, 138–39 (2d Cir. 1980) (finding that the government may not use a telescope to look into a person's home, even if the home is used for illegal activities).

95. *Skinner*, 690 F.3d at 777.

96. *See Katz v. United States*, 389 U.S. 347, 361 (1967).

97. *See United States v. Ellison*, 462 F.3d 557, 561 (6th Cir. 2006) (holding that a defendant has no reasonable expectation of privacy in a license plate).

detect his scent makes no difference. “Just as evidence in the plain view of officers may be searched without a warrant, evidence in the plain smell may be detected without a warrant.”⁹⁸ While a suspect’s scent in his own home may be subject to a reasonable expectation of privacy,⁹⁹ a public scent is not afforded the same protections.

There are other instances where police cannot obtain the signal emitted by a smartphone. A smartphone emits a signal when it makes a phone call. Such signal contains the voices and conversation between the two callers. Yet it is well established that police cannot listen to a suspect’s phone conversations, occurring through either a smartphone or a landline, without a warrant.¹⁰⁰ While police can obtain the phone numbers dialed by an individual without effectuating a search within the meaning of the Fourth Amendment,¹⁰¹ smartphone location information differs significantly from the numbers a caller dials. When dialing a phone number, a caller must affirmatively transmit that number to his phone service provider in order to complete the call. The Supreme Court has held that because this information is voluntarily disclosed to a third party, a caller no longer retains any privacy interest in it.¹⁰² But unlike the process that a person must engage in to dial a phone number, a smartphone user does not engage in any affirmative steps to transmit his location information to the phone service provider. Rather, the transmission of location information is only incidental to making a call. Additionally, the user does not make a choice of whether or not to transmit his or her location data when placing a phone call. The element of voluntary disclosure is lacking here, making location data more like a phone conversation than dialing a number.

III. A BETTER STANDARD TO USE FOR GPS TRACKING

This comment does not disagree with the majority’s holding in *Jones*. The common-law trespass analysis is a threshold question that courts have to address before deciding Fourth Amendment issues. But the Supreme

98. *United States v. Roby*, 122 F.3d 1120, 1125 (8th Cir. 1997) (internal citations omitted).

99. *Jardines v. Florida*, 73 So. 3d 34, 49–50 (Fla. 2011), *aff’d*, 133 S. Ct. 1409, 1416 (2013).

100. *See Alderman v. United States*, 394 U.S. 165, 175 (1969); *see also* 18 U.S.C. § 2518 (2012).

101. *Smith v. Maryland*, 442 U.S. 735, 745 (1979).

102. *Id.* at 744–45 (“This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.”); *see also United States v. Graham*, 846 F. Supp. 2d 384, 389 (D. Md. 2012) (finding a defendant does not have a legitimate expectation of privacy in historical cell site location records).

Court left open an important issue after *Jones*. A better test than the trespass analysis presented in *Jones* is whether society recognizes an individual's expectation of privacy in the GPS data of his smartphone as reasonable. If society recognizes such an expectation as reasonable then law enforcement agencies must obtain a warrant, supported by probable cause, in order to access and track such data. This proposal provides a bright-line standard that can be easily understood by law enforcement officers, treats all data emitted by a smartphone the same, provides an adequate and reasonable protection of an individual's privacy interests, and comports well with public policy by preventing the large scale tracking of individuals' movements.

A. Society Recognizes an Individual's Location Data as Private

If the *Katz* analysis is used over the physical trespass test, society must recognize a reasonable expectation of privacy in a person's GPS location data in order for it to be given Fourth Amendment protections. Telephones have long been considered to be private devices. The Omnibus Crime Control and Safe Streets Act of 1968¹⁰³ mandated that a warrant be obtained in order for the government to listen in on private phone conversations.¹⁰⁴ The extensive length of time that this safeguard has been in place would lead the average person to characterize transmissions by his phone as private. That GPS technology did not exist in 1968 does not change the conclusion: the Act was promulgated before text messaging existed, yet courts have held that individuals have a reasonable expectation of privacy in their text messages.¹⁰⁵ And even before the Act was put into place, the *Katz* court recognized the inherent privacy afforded to a person making a phone call: the government was prohibited from listening in to a person's phone call made from a telephone booth, even though the booth was in public.¹⁰⁶ Moreover, the Supreme Court held that "what [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."¹⁰⁷

Such is the case here. A person traveling in public necessarily makes his location known to all prying eyes. But even while carrying a smartphone, he does not make his GPS location data known to all. Rather, the data is only accessible to those with access to his smartphone. The lack of accessibility

103. 18 U.S.C §§ 2510–2522 (2012).

104. *Id.* § 2518.

105. *United States v. Finley*, 477 F.3d 250, 259 (9th Cir. 2007).

106. *Katz v. United States*, 389 U.S. 347, 351 (1967).

107. *Id.*

by the public to the individual's smartphone and GPS is consistent with the person preserving the data emitted by the device as private.

B. The Warrant Requirement Creates a Better Standard

This comment's argument, that society recognizes as reasonable the expectation of privacy in a person's smartphone location data, provides a bright-line standard that comports with the reasonable person's expectations. Such a standard benefits from the ease of administrability in two ways.

First, police officers, trial courts, and magistrate judges will have a clear answer about whether a warrant is required in order to track an individual's location. The warrant requirement exists so that evidence may be presented to a neutral and detached magistrate to review the evidence and need for a warrant, rather than a police officer making the decision. Police officers, who do not have the same legal training as judges, prosecutors, and defense attorneys, will engage in subjective decision making about the reasonableness of their location monitoring. This invites *ex post* litigation by both prosecutors and defendants about the reasonableness of the tracking. A bright-line rule would reduce much of the litigation about the proper duration of the monitoring and the officer's subjective beliefs. Of course, a defendant can still challenge the validity of a warrant on traditional grounds. But his challenge of the warrant would be measured against the well-known probable cause standard rather than the "relevant to an ongoing criminal investigation" standard of 18 U.S.C. § 2703(d).

Second, the signal emitted from a smartphone will no longer be treated as many different parts for Fourth Amendment purposes. The law treats voice, data, text messages, and location information transmitted by a smartphone differently,¹⁰⁸ although there is little reason to justify such a division. Even the reasonable person with no legal training is likely aware of the warrant requirement in order for police to initiate wiretaps. But this fictional person is unlikely to be aware of the fine contours between the different types of information the police can obtain from a phone without a warrant. An individual legitimately seeking to protect his personal information from prying eyes will be faced with many different standards. His phone calls will be protected under the Fourth Amendment, but not his location. The only way he can fully protect his location data is to power off

108. See *supra* notes 15–20 and accompanying text; see also *City of Ontario v. Quon*, 130 S. Ct. 2619, 2631 (2010) (allowing a government agency to review an employee's text messages); *United States v. Flores-Lopez*, 670 F.3d 803, 809–10 (7th Cir. 2012) (allowing police to read a suspect's text messages during a search incident to arrest).

his smartphone—an act which negates the primary purpose of owning and carrying a smartphone.¹⁰⁹

The differences between voice, data, and GPS locations on a smartphone are also fading. Many smartphones allow the user to engage in video chats through the phone's data network. These video chats contain features of both phone calls and internet use. Other smartphone applications may also utilize the user's GPS location to turn the phone into a "walkie-talkie."¹¹⁰ The end user is able to engage in a phone conversation, but the data is transmitted through different architecture. It is difficult to determine whether these "calls" should be subject to the traditional wiretap analysis, or should be accessible under the lesser "reasonable grounds" requirement of 18 U.S.C. § 2703. Under this comment's analysis, there is no need to draw fine distinctions between these different types of transmissions. All smartphone transmissions—voice, data, location, and combinations thereof—will be subject to the same warrant requirement. Should police wish to obtain and track any signal emitted from a smartphone, there will be only one standard that they must meet: the probable cause requirement of the Fourth Amendment.

C. Administrative Convenience & Limited Resources Do Not Justify a Lesser Standard

The majority in *Skinner* argued that requiring police officers to obtain a warrant in order to track a defendant's location data would place a higher burden on police officers, and that the law has never equated police efficiency with unconstitutionality.¹¹¹ While the law has never equated police efficiency with unconstitutionality, the converse is not necessarily true: just because a technique makes police officers more efficient does not make that technique constitutional.¹¹² Administrative convenience and

109. See generally Peter Maass & Megha Rajagopalan, *That's No Phone. That's My Tracker.*, N.Y. TIMES, July 13, 2012, at SR5 (internal citations omitted), available at http://www.nytimes.com/2012/07/15/sunday-review/thats-not-my-phone-its-my-tracker.html?_r=0 (discussing how smartphones causing the constant tracking of their users, and how to avoid such tracking).

110. See generally David Pogue, *Smartphone? Presto! 2-Way Radio*, N.Y. TIMES, Sept. 5, 2012, <http://www.nytimes.com/2012/09/06/technology/personaltech/zello-heyteell-and-voxer-make-your-smartphone-a-walkie-talkie-david-pogue.html?pagewanted=all> (discussing the growing use of walkie-talkie apps among smartphone users).

111. *United States v. Skinner*, 690 F.3d 772, 778 (6th Cir. 2012) (citing *United States v. Knotts*, 460 U.S. 276, 284 (1983)).

112. See *Kyllo v. United States*, 533 U.S. 27, 40 (2001) (holding the use of a thermal imaging device on a person's house as a search under the Fourth Amendment is unconstitutional without a warrant).

financial ease have never been valid reasons to sidestep constitutional requirements.¹¹³ Constitutional rights are the only bastion of protection that citizens enjoy against government. Dismissing them in the name of expenditure reduction ignores the protections given to citizens under the Fourth Amendment. Law enforcement agencies will be required to expend more resources in order to engage in physical surveillance of suspects¹¹⁴ or to obtain a warrant authorizing the tracking of a suspect's smartphone. Adopting such a rule will not send police officers to the technological Stone Age while allowing criminals to derive the benefits of such technologies. The availability of location data in smartphones is a relatively new innovation.¹¹⁵ That this technique is only recently developed supports the conclusion that police will not be unduly burdened by its restriction.¹¹⁶ Disallowing police officers to track smartphones will not reverse decades of police investigative techniques. This new standard used to analyze police location tracking information will not affect the ability of law enforcement agencies to engage in traditional physical surveillance techniques.

Criminals do not obtain any significant criminal benefits by using smartphones equipped with GPS devices. While smartphones can be used to coordinate illegal activities with other criminals, this is accomplished through phone calls and text messages rather than location data.¹¹⁷ Police who wish to track the calls and text messages sent from a smartphone are already subject to the stricter probable cause and warrant requirements. The smartphone's GPS device is only tangential to the purpose of the criminal enterprise. Refuting the *Skinner* court's concern, this does not present a scenario where criminals are taking advantage of technological changes "in order to . . . circumvent[] the justice system."¹¹⁸ The defendant in *Skinner*

113. See generally *Stanley v. Illinois*, 405 U.S. 645, 656 (1972) ("[T]he Constitution recognizes higher values than speed and efficiency.").

114. Physical surveillance does not exclude all technological advances. Cameras, radios, infrared devices, microphones, and similar technologies are all still viable options under this theory. This theory only seeks to exclude GPS tracking devices in smartphones.

115. The number of requests from law enforcement agencies to AT&T alone for location information has tripled from 2007 to present. See Lichtblau, *supra* notes 23–24 and accompanying text; see also Declan McCullagh, *Wireless Providers Side with Cops Over Users on Location Privacy*, CNET (Apr. 23, 2012, 10:20 AM), http://news.cnet.com/8301-31921_3-57418662-281/wireless-providers-side-with-cops-over-users-on-location-privacy/ (stating that only recently have states attempted to enact bills requiring a warrant for disclosure of such information; so far, legislative efforts have been unsuccessful).

116. To emphasize again, this comment is not arguing that this technique can *never* be used. To the contrary, this comment outlines when the technique is permissible.

117. See generally *Abuelhawa v. United States*, 556 U.S. 816, 822–23 (2009) (holding that the use of a cell phone in a drug trade does not "facilitate" the drug trade within the meaning of the Controlled Substances Act).

118. *United States v. Skinner*, 690 F.3d 772, 778 (6th Cir. 2012).

did not take advantage of the GPS device.¹¹⁹ The only attempt at circumventing the justice system, if any, occurred through the traditional use of smartphones—placing and receiving calls. The content of emails and phone calls are not subject to a lesser standard of protection than the probable cause warrant requirement because both the sinner and the saint use email and smartphones; it would be incongruous to subject GPS devices to a lesser standard simply because criminals may use smartphones equipped with GPS devices.

Finally, the increased burden on law enforcement is not so substantial as to make GPS tracking extinct. When presenting a warrant request for a wiretap, officers may also request to track the location of a smartphone. It is unlikely that this minor additional burden would deter a warrant application. Should a magistrate find that there is probable cause to authorize a wiretap, she may also find probable cause to authorize the tracking of that smartphone. Of course, the magistrate may also reject the request to track the location of a smartphone while authorizing a wiretap. This presents the precise situation that this comment advocates for: the existence of a reasonable expectation of privacy in an individual's smartphone location data that is subject to Fourth Amendment considerations.

D. Widespread Location Monitoring Could Have Extreme Repercussions

This comment's proposal should be adopted in order to prevent widespread monitoring of individuals' locations. If there is a reasonable expectation of privacy in an individual's GPS location data, then police will not be able to enact dragnet style operations that would capture and record a person's aggregate movements. Average people do not "expect that their movements will be recorded and aggregated."¹²⁰ To know someone's whereabouts is to know who he is: "GPS data can reveal whether a person is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, [or] an outpatient receiving medical treatment."¹²¹ A person who knows that his whereabouts are constantly subject to tracking and recording will be reluctant to engage in many daily activities. A visit to the doctor's office to obtain embarrassing test results could become public knowledge.

119. *Id.*

120. *United States v. Jones*, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring).

121. Peter Maass & Megha Rajagopalan, *That's No Phone. That's My Tracker.*, N.Y. TIMES, July 13, 2012, at SR5 (internal citations omitted), available at http://www.nytimes.com/2012/07/15/sunday-review/thats-not-my-phone-its-my-tracker.html?_r=0.

In *Jones*, Justice Sotomayor expressed such concerns about widescale monitoring: “[a]wareness that the Government may be watching chills associational and expressive freedoms.”¹²²

Numerous other courts have also expressed concerns over wide dragnet type programs that could monitor the locations of large numbers of individuals.¹²³ These courts have recognized a distinction between physical surveillance by police, and widespread GPS tracking. While police may engage in around-the-clock physical surveillance of a suspect, achieving the same result through GPS location tracking presents a different problem. In *Jones*, Justice Sotomayor cautioned that “because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: ‘limited police resources and community hostility.’”¹²⁴ There is an implicit limit on ordinary police surveillance: the inability of police officers to be everywhere at once. Police departments only have a limited number of officers, and so they must concentrate their efforts on the most important concerns. A police officer who is assigned to around-the-clock surveillance of a suspect necessarily gives up the ability to conduct the same kind of surveillance of another suspect at the same time. Under these constraints, it would be an unreasonable waste of time for police officers to focus their efforts on an individual without some heightened degree of suspicion.

But concerns of limited resources are eroded when police can use technology to track a suspect. GPS tracking devices are available for a fraction of the cost of training and deploying an officer.¹²⁵ Costs are further reduced when the GPS device being tracked is not being deployed by police, as in the *Jones* case, but is built in to an individual’s smartphone.

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

123. *See, e.g., id.* at 954; *United States v. Knotts*, 460 U.S. 276, 284 (1983) (“[I]f such dragnet type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable.”); *Skinner*, 690 F.3d at 780 (“There may be situations where police, using otherwise legal methods, so comprehensively track a person’s activities that the very comprehensiveness of the tracking is unreasonable for Fourth Amendment purposes.”); *United States v. Pineda-Moreno*, 617 F.3d 1120, 1124 (9th Cir. 2010) (Kozinski, J., dissenting from the denial of rehearing en banc) (“By holding that this kind of surveillance doesn’t impair an individual’s reasonable expectation of privacy, the panel hands the government the power to track movements of every one of us, every day of our lives.”).

124. *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) (quoting *Illinois v. Lidster*, 540 U.S. 419, 426 (2004)).

125. *Id.* (stating that “GPS monitoring is cheap in comparison to conventional surveillance techniques”).

Even with the charges from phone service providers,¹²⁶ police can obtain smartphone location information for relatively low cost as compared to the cost of twenty-four hour physical surveillance by police officers. “The net result is that GPS monitoring . . . mak[es] available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track.”¹²⁷ With the possibility of widespread tracking by government agencies no longer just a science fiction dream, a higher level of protection for an individual’s location data is needed to safeguard personal liberties.

CONCLUSION

The *Katz* standard of evaluating the constitutionality of police action should be adopted for GPS location tracking in order to better align the purposes of the Fourth Amendment with the reasonable expectations of society. Society recognizes a reasonable expectation of privacy in an individual’s location data as emitted by his smartphone. Recognizing this expectation as legitimate will require police to obtain a warrant in order to track a person’s smartphone through the phone’s GPS device.

Given the Supreme Court’s recent decision in *Jones*, and the number of issues it left open, it is likely that circuit courts will split on the constitutionality of location monitoring by police under § 2703. Without action by the Congress, state legislatures, or from the Supreme Court itself, it will be difficult to prevent such a split. The Supreme Court stated that it would address the hypothetical threat of warrantless tracking without a physical trespass when such a case arose.¹²⁸ At least one such case, *Skinner*, already exists, and given the Sixth Circuit’s favorable treatment of the police conduct there, it does not take a crystal ball to predict that similar cases will arise. Police will continue to use this technique, given its blessing by courts, until they are constrained by law or by the Supreme Court. The Supreme Court should act sooner rather than later to address this problem. If these dragnet techniques become commonplace, Congress or the Supreme Court may be more hesitant to put an end to such procedures.

126. See Greenberg, *supra* notes 21–22 and accompanying text; Lichtblau, *supra* note 23 and accompanying text.

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

128. *Id.* at 954.