Oklahoma Law Review

Volume 70 | Number 4

2018

United States v. Lambis: A Good Call for Cellphones, Cell-site Simulators, and the Fourth Amendment

Kathryn E. Gardner

United States v. Lambis: A Good Call for Cellphones, Cell-site Simulators, and the Fourth Amendment

I. Introduction

Perhaps when you were a child, you liked to play this classic twist on "hide and seek" with your friends. The "seeker" would count aloud to some designated number while the "hiders" scurried about and jockeyed for the best hiding position. Once the seeker rounded up a few of the other hiders, the hiders would then begin to provide the seeker with clues to your location—shouting "warmer" when the seeker was nearing your spot or taunting "freezing cold" when the seeker was off searching another room. Eventually the game would come to an end when you heard your friends shriek, "boiling hot!" as the curtain you were cowering behind was suddenly ripped open. Now imagine a technological tool equivalent to your childhood friends that relied on your own cellphone to provide hints to your location. If you are one of the ninety-two percent of American adults who own a cellphone of some kind, this is understandably concerning.[1]

Cell-site simulators—also referred to as "StingRays," "Hailstorms," "TriggerFish," or "IMSI catchers"—are powerful surveillance tools that enable law enforcement officers and agencies to pinpoint a cellphone's location within a few yards.[2] Just as someone's shouts would drown out another's whisper, cell-site simulators drown out the signals of legitimate cell towers and force cellphones nearby to connect with them instead.[3] Once connected, the information captured by cell-site simulators can range from real-time location data to the content of communications.[4] Because

1. Monica Anderson, *Technology Device Ownership: 2015*, PEW RES. CTR., Oct. 29, 2015, http://www.pewinternet.org/files/2015/10/PI_2015-10-29_device-ownership_FINAL.pdf.

2. United States v. Lambis, 197 F. Supp. 3d 606, 609 (S.D.N.Y. 2016), *appeal withdrawn*, No. 16-3146, 2017 U.S. App. WL 4127919 (2d Cir. Mar. 13, 2017).; *Cell-Site Simulators/IMSI Catchers*, ELECTRONIC FRONTIER FOUND. (last visited Mar. 23, 2017), https://www.eff.org/sls/tech/cell-site-simulators.

3. *Cell-Site Simulators/IMSI Catchers*, *supra* note 2. "Cellular networks are distributed over geographic areas called 'cells.'" *Id.* "Each cell is served by [a tower], also known as a cell-site." *Id.* "Your [cell]phone naturally connects with the closest [cell-site] to provide you with service as you move" around. *Id.* Essentially, cell-site simulators trick your cellphone into thinking they are cell-sites. *Id.*

4. *Id.* Primarily, cell-site simulators target four types of information: "(1) identifying information about the [cellphone] like the International Mobile Subscriber Identity (IMSI) number"; (2) "metadata about calls like who you are dialing and duration of call"; (3) "the content of SMS and voice calls"; and (4) "data usage, such as websites visited." *Id.*

cellphones are constantly communicating with cell towers even if they are safely tucked away in an owner's purse or pocket, the only way to protect oneself from susceptibility to a nearby cell-site simulator is to shut the cellphone off completely.[5] Cell-site simulators thus operate in a dragnet fashion—scooping up data and information not only from the targeted cellphone, but also from all cellphones that happen to be operating in the vicinity.[6]

This Note will examine *United States v. Lambis*, a recent decision by the United States District Court for the Southern District of New York, and discuss the decision's unfavorable treatment of the warrantless use of cell-site simulators by law enforcement officers and agencies.[7] Part I provided a brief introduction to cell-site simulator technology.[8] Part II examines the landmark decisions that have shaped current Fourth Amendment jurisprudence, especially those doctrines relied on by the district court in the *Lambis* opinion.[9] Part III describes the circumstances surrounding the events that led to *United States v. Lambis*,[10] while Part IV discusses the district court's decision.[11] Part V analyzes the district court's unique application of Fourth Amendment jurisprudence to cutting-edge technology,[12] and argues that courts across the country should adopt a similar line of reasoning. Finally, Part VI draws conclusions regarding the current state of privacy and protections afforded by the Fourth Amendment and emphasizes why a novel approach like that found in *United States v. Lambis* better safeguards the rights central to the foundations of liberty and democracy.[13]

---

5. *Cell-Site Simulators: Frequently Asked Questions: Can I Prevent Having My Data Captured by Cell Site Simulators?*, ELECTRONIC FRONTIER FOUND. (last visited Mar. 23, 2017), https://www.eff.org/node/89287#faq-Can-I-prevent-having-my-data-captured-by-cell-site-simulators?.

6. *Cell-Site Simulators: Frequently Asked Questions: How Does It Work?*, ELECTRONIC FRONTIER FOUND. (last visited Mar. 23, 2017), https://www.eff.org/node/89287#faq-How-does-it-work?.

7. *See Lambis*, 197 F. Supp. 3d 606.

8. *See Cell-Site Simulators/IMSI Catchers,* supra note 2.

9. *See Lambis*, 197 F. Supp. 3d at 609-16.

10. *See id.* at 608-09.

11. *See id.* at 609-16.

12. *See id.*

13. *See id.*

II. Law Before the Case

A. The Fourth Amendment's Guarantee Against Unreasonable Searches

What began as a get-rich-quick scheme for one individual quickly ballooned into a landmark Fourth Amendment case: *Katz v. United States*.[14] Charles Katz was the target of a Federal Bureau of Investigation (FBI) sting operation in which FBI agents attached an electronic eavesdropping device to the outside of a telephone booth Katz was regularly using to transmit wagering information across the country.[15] Katz was subsequently arrested, charged, and convicted; he later challenged his conviction, arguing that the electronic eavesdropping device and its recordings violated his Fourth Amendment rights and that the evidence gathered by its use should be suppressed.[16]

The Fourth Amendment provides, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches . . . shall not be violated."[17] Traditionally, this right was guarded via application of the physical trespass doctrine, whereby physical intrusions into a constitutionally protected area to obtain information were regarded as unreasonable searches.[18] This theory has made a resurgence in recent years following the Supreme Court's decision in *United States v. Jones*.[19] There, the Court held that installing a global positioning system (GPS) device on the undercarriage of a vehicle and using the device to monitor the vehicle's movements over an extended period of time constituted an unreasonable search under the Fourth Amendment because the government had usurped the individual's property.[20]

The more modern doctrine, however, was first described in Justice Harlan's concurrence in *Katz v. United States* and is composed of two prongs.[21] If an individual can show that (1) he or she had a subjective

---

14. 389 U.S. 347 (1967).

15. *Id.* at 348.

16. *Id.*

17. U.S. CONST. amend. IV.

18. *See* United States v. Jones, 565 U.S. 400, 404-06 (2012) (discussing the origin of Fourth Amendment jurisprudence).

19. *See id.*

20. *Id.* at 404 ("We hold that the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search.'").

21. *Katz*, 389 U.S. at 361 (Harlan, J., concurring) ("My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation

expectation of privacy in what was searched, and (2) that society is prepared to recognize that individual's expectation as reasonable, then the search was unreasonable.[22] Because the first prong is more easily satisfied due to its subjective nature, the Supreme Court more often focuses on whether there was a reasonable expectation of privacy in what was searched to determine the reasonableness of the intrusion and whether it comports with the Fourth Amendment.[23]

To utilize the physical trespass doctrine when dealing with electronic surveillance would be an exercise in futility, as no physical intrusion is actually involved in the invasion.[24] The reasonable expectation of privacy test from *Katz v. United States*[25] is therefore the appropriate analysis for searches comprised solely of electronic surveillance—as confirmed by the Supreme Court in *Jones*.[26] If government conduct invades a reasonable expectation of privacy,[27] then the conduct is considered an unreasonable search for Fourth Amendment purposes.[28] Under this standard, Katz's challenge was successful and the recordings from the electronic eavesdropping device were suppressed.[29]

---

be one that society is prepared to recognize as 'reasonable.'"). This two-step test described by Justice Harlan, though applied in intervening cases, was not formally ratified by the Court until 1979. *See* Smith v. Maryland, 442 U.S. 735, 740 (1979).

22. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

23. *Smith*, 442 U.S. at 740 ("Consistently with *Katz*, this Court uniformly has held that the application of the Fourth Amendment depends on whether the person invoking its protection can claim a 'justifiable,' a 'reasonable,' or a 'legitimate expectation of privacy' that has been invaded by government action.") (citing Rakas v. Illinois, 439 U.S. 128 (1977); United States v. Chadwick, 433 U.S. 1, 7 (1977); United States v. Miller, 425 U.S. 435, 442 (1976); United States v. Dionisio, 410 U.S. 1, 14 (1973); Couch v. United States, 409 U.S. 322, 335–36 (1973); United States v. White, 401 U.S. 745, 752 (1971) (plurality opinion); Mancusi v. DeForte, 392 U.S. 364, 368 (1968); Terry v. Ohio, 392 U.S. 1, 9 (1968)).

24. *See Jones*, 565 U.S. at 411-12.

25. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

26. *Jones*, 565 U.S. at 411 ("Situations involving merely the transmission of electronic signals without trespass would remain subject to *Katz* analysis.").

27. For example, the Supreme Court has held that searching the digital contents of a cellphone incident to arrest and without the authorization of a warrant violated the Fourth Amendment. *See* Riley v. California, 134 S. Ct. 2473, 2477 (2014).

28. *Smith*, 442 U.S. at 740.

29. *Katz*, 389 U.S. at 359.

B. Which Test to Use in Light of Cell-site Simulators? Making Sense of the Supreme Court's Myriad of Fact-Intensive Rules

Since the Supreme Court has yet to decide whether the warrantless use of a cell-site simulator invades a reasonable expectation of privacy and is therefore an unreasonable search within the meaning of the Fourth Amendment, it is important to consider the myriad of fact-intensive rules that inform the Supreme Court's reasoning in such matters.

1. Knotts*,* Karo*, and Searches Within the Home*

One oft-quoted rationale of the Court's decision in *Katz v. United States* is that "the Fourth Amendment protects people, not places."[30] This radical departure from the physical trespass doctrine meant that anyone could enjoy an expectation of privacy wherever he or she may go, untethered from previous ideas that protection should singularly be afforded to places such as a home.[31] Even under modern Fourth Amendment jurisprudence, however, an individual's home is still accorded the highest degree of protection when compared to an individual's car, container, or the like.[32] This elevated level of protection is afforded because the very core of the Fourth Amendment entitles an individual to "retreat into his [or her] own home and there be free from unreasonable governmental intrusion."[33] Absent a few well-delineated exceptions, the search of a home typically requires a warrant; without one, the search is presumptively unreasonable.[34] This is so because the search warrant requirement was designed primarily "to interpose a 'neutral and detached magistrate' between the citizen and 'the officer engaged in the often competitive enterprise of ferreting out crime.'"[35]

Two cases—*United States v. Knotts*[36] and *United States v. Karo*[37]—illustrate this principle in a striking manner. Both cases involved "beepers" surreptitiously installed by law enforcement in cans of chemicals expected to later be used in drug manufacturing.[38] The beepers allowed law

30. *Id.* at 351.
31. *See id.*
32. *See id.* at 359.
33. Silverman v. United States, 365 U.S. 505, 511 (1961).
34. United States v. Karo, 468 U.S. 705, 714-15 (1984).
35. *Id.* at 717 (quoting Johnson v. United States, 333 U.S. 10, 14 (1948)).
36. 460 U.S. 276 (1983).
37. 468 U.S. at 705.
38. *Knotts*, 460 U.S. at 276; *Karo*, 468 U.S. at 705.

enforcement to track the movement of the cans over time and across geographic areas.[39]

In *Knotts*, law enforcement tracked the cans as they were placed into a vehicle and traveled along public roads.[40] While police were able to maintain visual contact for most of the journey, they had to rely on the beeper's capabilities to ascertain the exact resting place of the cans once the journey had come to an end outside a cabin owned by Knotts.[41] Because there was no indication that the beeper was used to gather information regarding the private area inside Knotts's cabin, the Supreme Court ruled that there was no reasonable expectation of privacy in one's movements from one place to another when traveling on "public thoroughfares."[42]

In *Karo*, however, law enforcement tracked the cans as they were sold, moved between multiple residences and commercial storage lockers, and eventually came to rest inside a private residence.[43] This critical distinction—where the cans came to rest—led the Supreme Court to draw a definite rule that "[t]he monitoring of a beeper in a private residence, a location not opened to visual surveillance, violates the Fourth Amendment rights of those who have a justifiable interest in the privacy of the residence."[44] In light of both cases, it seems the Supreme Court would likely find a search unreasonable where an electronic tracking device is used to reveal information from within a home.

2. Kyllo v. United States *and Technology Not Commonly Available to the Public*

In *Kyllo v. United States*, the Supreme Court added another interesting piece to the Fourth Amendment puzzle.[45] After *Knotts* and *Karo* clarified that the Supreme Court was willing to draw a line between tracking technology used within the home and that used outside the home, the *Kyllo* Court took a step further to draw a "firm but also bright" line at the entrance of the home in order to protect it from all types of warrantless surveillance.[46]

---

39. *Knotts*, 460 U.S. at 276; *Karo*, 468 U.S. at 705.

40. *Knotts*, 460 U.S. at 276.

41. *Id.* at 279.

42. *Id.* at 276 ("A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements.").

43. *Karo*, 468 U.S. at 705.

44. *Id.* at 706.

45. 533 U.S. 27 (2001).

46. *Kyllo*, 533 U.S. at 40.

Danny Kyllo's home was the subject of an investigation after law enforcement agents became suspicious that he was growing marijuana inside.[47] Agents used a thermal imaging device to record heat emanating from Kyllo's home.[48] The device revealed an unusual amount of heat radiating from his garage when compared to the rest of his home.[49] Agents then used this information to obtain a search warrant, which ultimately aided in their discovery of a large amount of marijuana plants.[50] The Supreme Court, however, held that the use of the thermal imaging device was an unreasonable search within the meaning of the Fourth Amendment.[51] In reaching its decision, the Supreme Court relied heavily on the fact that the technology employed by the agents was not in use by the general public.[52] Taking the rationale of *Knotts* and *Karo* one step further, the Supreme Court carved out yet another Fourth Amendment protection whereby a search occurs when sense-enhancing technology that is not in general public use is utilized to obtain any information regarding the interior of a home that could not otherwise have been obtained without physical intrusion into a constitutionally protected area.[53]

3. Smith v. Maryland *and the Third Party Doctrine*

In light of modern technological advances, the "third party doctrine" is one area of Fourth Amendment jurisprudence that has a rather chilling bright-line rule.[54] In *Smith v. Maryland*, local police installed a pen register

47. *Id.* at 29.

48. *Id.* In order to grow marijuana indoors, a large amount of light is needed for the plants to undergo photosynthesis, which results in an abnormally large heat signature. *Id.*; *see also* Gina S. Warren, *Regulating Pot to Save the Polar Bear: Energy and Climate Impacts of the Marijuana Industry*, 40 COLUM. J. ENVTL. L. 385, 403-04 (2015).

49. *Kyllo*, 533 U.S. at 30.

50. *Id.*

51. *Id.* at 40.

52. *Id.* at 34-35.

53. *Kyllo*, 533 U.S. at 40 ("Where . . . the Government uses a device that is not in general public use, to explore details of [a private] home that would previously have been unknowable without physical intrusion, the surveillance is a [Fourth Amendment] 'search' and is presumptively unreasonable without a warrant.").

54. *See* United States v. Miller, 425 U.S. 435, 443 (1976) ("This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."); *see also* Smith v. Maryland, 442 U.S. 735, 743-44 (1979) ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.").

on telephone company property to record all the numbers dialed from a particular telephone in order to trace the source of menacing calls made to a robbery victim.[55] Shortly thereafter, Michael Smith was identified as the culprit.[56] At trial, Smith sought to suppress "all fruits derived from the pen register" because the police had failed to obtain a warrant before its installation and therefore violated his reasonable expectation of privacy in the telephone numbers he dialed.[57] Like the trial court, the Supreme Court, rejected Smith's argument.[58]

In what is known as the third party doctrine, the Supreme Court has consistently recognized that individuals have no reasonable expectation of privacy in the information they voluntarily provide to third parties, such as telephone service providers.[59] Rather,

> The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. . . . [T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[60]

The Supreme Court's decision in *Smith v. Maryland*, however, was handed down in 1979.[61] Is such a bright-line rule still appropriate in light of modern technological advances? At least one Justice of the United States Supreme Court is ready to ask the question.[62]

---

55. *Smith*, 442 U.S. at 737.

56. *Id.*

57. *Id.*

58. *Id.* at 745-46 (concluding Smith did not entertain an actual expectation of privacy in the phone numbers he dialed and that even if he did, his expectation was not legitimate).

59. *E.g.*, *id.*; United States v. Miller, 425 U.S. 435, 442-44 (1976); Couch v. United States, 409 U.S. 322, 335-36 (1973); United States v. White, 401 U.S. 745, 752 (1971); Hoffa v. United States, 385 U.S. 293, 302 (1966); Lopez v. United States, 373 U.S. 427 (1963).

60. *Miller*, 425 U.S. at 443 (citations omitted).

61. 442 U.S. at 735.

62. *See* United States v. Jones, 565 U.S. 400, 413-18 (2012) (Sotomayor, J., concurring).

C. Consequences of Multiple Tests: Confusion in the Lower Courts

Unsure of what line of reasoning to follow, courts across the country have issued a dizzying series of opinions regarding cell-site simulators and other related technology. For example, the Fourth Circuit recently held that the government did not violate the Fourth Amendment when it obtained historical cell-site location information from a cellphone provider without a warrant because the defendants had voluntarily conveyed that information to a third party by making and receiving calls and texts on their cellphones.[63] Yet, the Third Circuit disagrees with the idea that such actions constituted a voluntary conveyance of location information.[64] And the Fifth Circuit would draw a dispositive line based on whether it is the government collecting the information or "whether it is a third party, of its own accord and for its own purposes, recording the information."[65]

Similar to the Third Circuit, a Maryland court chose to simply reason that "people have a reasonable expectation that their cell phones will not be used as real-time tracking devices by law enforcement."[66] Likewise, the Florida Supreme Court has concluded that society is prepared to recognize a subjective expectation of privacy in location signals transmitted by cellphones.[67] If anything can be demonstrated by the confusion among the lower courts, it is that there is a definitive need for a clear directive on how to apply the Fourth Amendment to cutting-edge technology such as cell-site

63. United States v. Graham, 824 F.3d 421, 427 (4th Cir. 2016) (en banc). Similarly, the Sixth Circuit recently held the government did not conduct a search for Fourth Amendment purposes when it obtained business records from the defendants' wireless carriers that contained historical cell-site location information. United States v. Carpenter, 819 F.3d 880, 890 (6th Cir. 2016). The Eleventh Circuit has also held that obtaining historical cell tower location information via a third-party telephone company's business records did not violate the defendant's Fourth Amendment rights. United States v. Davis, 785 F.3d 498, 518 (11th Cir. 2015).

64. *In re* the Application of the United States for an Order Directing a Provider of Elec. Comm'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 317-18 (3d Cir. 2010) ("A cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way.").

65. *In re* United States for Historical Cell Site Data, 724 F.3d 600, 610 (5th Cir. 2013).

66. State v. Andrews, 134 A.3d 324, 327 (Md. Ct. Spec. App. 2016).

67. Tracey v. State, 152 So. 3d 504, 526 (Fla. 2014) ("[W]e conclude that such a subjective expectation of privacy of location as signaled by one's cell phone—even on public roads—is an expectation of privacy that society is now prepared to recognize as objectively reasonable under the *Katz* 'reasonable expectation of privacy' test.").

simulators. One case in particular, *United States v. Lambis*, just might provide an answer.[68]

III. Statement of the Case

A. Facts

United States v. Lambis centers around a cellphone.[69] In the course of an international drug trafficking investigation, the Drug Enforcement Administration (DEA) came to suspect Hugo Fernando Valenzuela Gomez of brokering the movement of thousands of kilograms of narcotics through South America, Central America, Europe, and the United States.[70] Accordingly, the DEA obtained judicial authorization to tap Gomez's communications.[71] In the New York area, Gomez and his associates allegedly possessed a large amount of heroin.[72] To improve the quality of the heroin, Gomez needed hydrochloric acid.[73] "On or about August, 15, 2015, the DEA intercepted a BlackBerry exchange" between Gomez and an associate that read, "646 894 4983 'patilla.' It's for the liquids."[74]

The cellphone belonging to "Patilla" quickly morphed into the target of the DEA's investigation.[75] Hoping to gather more information, the DEA sought a warrant for the targeted cellphone's pen register information and cell site location information (CSLI).[76] The pen register information—"a record from the service provider" that includes telephone numbers dialed from the cellphone—allowed the DEA to approximate a network of criminal associates using the targeted cellphone.[77] Even more illuminating, the CSLI—a record from the service provider that includes location

68. United States v. Lambis, 197 F. Supp. 3d 606 (S.D.N.Y. 2016), *appeal withdrawn*, No. 16-3146, 2017 U.S. App. WL 4127919 (2d Cir. Mar. 13, 2017).

69. *Id.* at 608.

70. The Government's Opposition to Defendant's Motion to Suppress Evidence, Exhibit A at 11-12, United States v. Lambis, 197 F. Supp. 3d 606 (S.D.N.Y. 2016) (No. 1:15-cr-00734).

71. *Id.* at 11.

72. *Id.* at 12.

73. *Id.* Based on her training, experience, and involvement in this particular investigation, DEA Special Agent Kathryn Glover alleged that hydrochloric acid is commonly used, often in large quantities, to purify lower-quality heroin, also referred to as "street" heroin. *Id.*

74. *Id.*

75. *Id.* at 13.

76. United States v. Lambis, 197 F. Supp. 3d 606, 608 (S.D.N.Y. 2016), *appeal withdrawn*, No. 16-3146, 2017 U.S. App. WL 4127919 (2d Cir. Mar. 13, 2017).

77. *Id.*

information derived from "pings" sent by the cellphone to nearby cell sites—allowed the DEA to approximate the general location of the targeted cellphone based on its previous use.[78]

Using the CSLI, DEA agents were able to determine the approximate location of the targeted cellphone within a few blocks.[79] Within this small area of the Washington Heights neighborhood of New York City, however, were several apartment complexes, each containing a multitude of units.[80] The CSLI was simply not precise enough to trace the targeted cellphone back to any single complex or unit.[81] Failing to first seek the authorization of a warrant, the DEA deployed a technician with a cell-site simulator in the location approximated by the CSLI in order to further narrow the targeted cellphone's location.[82]

Calculating the strength of the pings intercepted on their way to the nearest cell tower, the technician was able to trace the targeted cellphone to a specific apartment complex.[83] The technician then entered the apartment building and began to walk the halls until he located a specific apartment unit—home to Raymond Lambis—where the strength of the pings emanating was the greatest.[84] That evening, DEA agents knocked on the door.[85] After being let into the apartment, the DEA obtained consent from Lambis to search his bedroom.[86] Ultimately, the search yielded narcotics and paraphernalia that became the crux of the Government's case, including cocaine, three digital scales, empty ziplock bags, an X-Acto knife, and a large plastic bag containing approximately eight cellphones.[87]

B. Procedural History and Issue

After his arrest, Raymond Lambis was charged with one count of conspiracy to distribute a controlled substance—a charge that carries a prison sentence of five to forty years upon conviction.[88] Lambis sought to have the narcotics and drug paraphernalia suppressed and was ultimately

78. *Id.* at 608-09.
79. *Id.* at 609.
80. *Id.*
81. *Id.*
82. *Id.*
83. *Id.*
84. *Id.*
85. *Id.*
86. *Id.*
87. Complaint at 3, United States v. Lambis, 197 F. Supp. 3d 606 (S.D.N.Y. 2015) (No. 1:15-cr-00734).
88. *Id.* at 1; 21 U.S.C. § 841(b)(1)(B) (2012).

successful by arguing that the DEA's warrantless use of a cell-site simulator to locate his cellphone within his apartment violated his Fourth Amendment right to be free from unreasonable searches.[89]

IV. Decision

To begin its analysis, the Southern District of New York first emphasized the Fourth Amendment's command of reasonableness.[90] A few sentences later, however, the court pointedly reemphasized that warrantless searches are per se unreasonable barring a few narrow exceptions.[91] Continuing, the court then highlighted the home's "special significance under the Fourth Amendment" before diving into current case law.[92]

The district court first turned to the seminal Supreme Court case *Kyllo v. United States*.[93] The court was especially concerned that the technology presently before it in *Lambis*[94] was the exact kind of technology the Supreme Court warned of in *Kyllo*.[95] Comparing cellphone pings to heat emanating from a home, the district court observed that neither were readily observable to "anyone who wanted to look" without the use of a cell-site simulator or thermal imaging device.[96] Just as the thermal imaging device in *Kyllo* revealed "details of the home that would previously have been unknowable without physical intrusion,"[97] so too did the cell-site simulator.[98]

Rejecting the Government's argument that the information gathered from the cell-site simulator was only the targeted cellphone's location and not intimate details "such as 'what hour each night the lady of the house takes

---

89. *Lambis*, 197 F. Supp. 3d at 616.

90. *Id.* at 609.

91. *Id.*

92. *Id.*

93. *Id.*; 533 U.S. 27 (2001). To reiterate, the Supreme Court in *Kyllo* held that, "[w]here . . . the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant." *Id.* at 40. In part, the Supreme Court rejected the Government's argument because distinguishing between "'off-the-wall' observations and 'through-the-wall surveillance'" would leave the "homeowner at the mercy of advancing technology." *Id.* at 35; *see supra* Section II.B.2.

94. *Lambis*, 197 F. Supp. 3d at 609-10.

95. *See Kyllo*, 533 U.S. at 35-36.

96. *Lambis*, 197 F. Supp. 3d at 610 (quoting United States v. Knotts, 460 U.S. 276, 281 (1983)).

97. *Kyllo*, 533 U.S. at 40.

98. *Lambis*, 197 F. Supp. 3d at 610.

her daily sauna and bath,'"[99] the district court relied on a Second Circuit opinion that found such distinctions inappropriate even if they solely revealed "the presence or absence of narcotics."[100] In the case of cellphones, the court concluded that an electronic search was "far more intrusive . . . because, unlike narcotics, cell phones are neither contraband nor illegal. In fact, they are ubiquitous."[101] Again similar to the thermal imaging device in *Kyllo*, the court noted that cell-site simulators are not a device in general public use.[102] Thus, the DEA's warrantless use of the cell-site simulator to locate Lambis's apartment was an unreasonable search within the meaning of the Fourth Amendment.[103]

The district court also supported its reasoning[104] with another Supreme Court case of monumental importance—*United States v. Karo*.[105] In *Karo*, the Supreme Court held that, "the monitoring of a beeper in a private residence, a location not opened to visual surveillance, violates the Fourth Amendment rights of those who have a justifiable interest in the privacy of the residence."[106] In so holding, the Supreme Court spurned the Government's argument that if requisite justification exists on the facts to support "that monitoring the beeper" wherever it may go would "produce evidence of criminal activity," the government's conduct should not constitute a search.[107] Like the Supreme Court in *Karo*,[108] the district court in *Lambis*[109] strongly undercut this contention, fearing the exception would swallow the rule as the primary reason for the warrant requirement is to "interpose a 'neutral and detached magistrate' between the citizen and 'the officer engaged in the often competitive enterprise of ferreting out crime.'"[110] Even though the DEA believed that by using the cell-site

99. *Id.* (quoting *Kyllo*, 533 U.S. at 38).

100. *See* United States v. Thomas, 757 F.2d 1359, 1366-67 (2d Cir. 1985) (holding that a canine sniff constitutes a search under the Fourth Amendment "when employed at a person's home").

101. *Lambis*, 197 F. Supp. 3d at 610.

102. *Id.*

103. *Id.* at 611.

104. *Id.*

105. 468 U.S. 705 (1984).

106. *Id.* at 714.

107. *Id.* at 717.

108. *Id.* (recognizing that "[w]arrantless searches are presumptively unreasonable").

109. *Lambis*, 197 F. Supp. 3d at 611 ("[E]ven though the DEA believed that the use of the cell-site simulator would reveal the location of a phone associated with criminal activity, the Fourth Amendment requires the Government to obtain a warrant from a neutral magistrate to conduct that search.").

110. *Karo*, 468 U.S. at 717 (quoting Johnson v. United States, 333 U.S. 10, 14 (1948)).

simulator it would pinpoint the location of a cellphone involved in criminal activity, the district court stressed that it was the role of a neutral magistrate to make the call.[111] The court also pointed out that whatever warrants were obtained in the course of the investigation (namely the warrants for pen register information and CSLI information), the DEA clearly exceeded their scope by obtaining information via the cell-site simulator, which was not contemplated by the original warrant application.[112]

Turning its attention to another relevant Fourth Amendment concern, the district court discussed the third party doctrine.[113] Disregarding altogether whether or not the third party doctrine is best suited for the digital age,[114] the district court went straight to *Smith v. Maryland*.[115] In *Smith*, a case involving pen registers, the Supreme Court reasoned that the third party doctrine applies when a party, "voluntarily turns over [information] to third parties."[116] The district court, however, made findings based on two observations that "the location information detected by a cell-site simulator is different in kind from pen register information: it is neither initiated by the user nor sent to a third party."[117]

First, "cell phone users do not actively submit their location information" to service providers.[118] Rather, cellphones automatically send signals to nearby cell towers to maintain a connection to the network, and other courts[119] have concluded that these passive signals do not trigger the third

111. *Lambis*, 197 F. Supp. 3d at 611.

112. *Id.*

113. *Id.* at 614-16.

114. *Id.* at 614.

115. 442 U.S. 735 (1979).

116. *Id.* at 744.

117. *Lambis*, 197 F. Supp. 3d at 614.

118. *Id.* at 615 (quoting State v. Andrews, 134 A.3d 324, 325 (Md. Ct. Spec. App. 2016)).

119. *See In re* the Application of the United States for an Order Directing a Provider of Elec. Comm'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 317-18 (3d Cir. 2010) ("A cell phone customer has not "voluntarily" shared his location information with a cellular provider in any meaningful way."); Tracey v. State, 152 So.3d 504, 526 (Fla. 2014) ("[W]e conclude that such a subjective expectation of privacy of location as signaled by one's cell phone—even on public roads—is an expectation of privacy that society is now prepared to recognize as objectively reasonable under the *Katz* 'reasonable expectation of privacy' test."); State v. Earls, 70 A.3d 630, 641 (N.J. 2013) (citations omitted) ("When people make disclosures to phone companies and other providers to use their services, they are not promoting the release of personal information to others. . . . Instead, they can reasonably expect that their personal information will remain private.").

party doctrine.[120] Furthermore, the district court pointed out that cell-site simulators involve an additional layer of involuntariness as they force all cellphones in the nearby area to repeatedly transmit their signals until a location is derived.[121]

Second, cell-site simulators do not involve a third party because "[t]he question of *who* is recording [the] information"—a third party or the government—is dispositive.[122] By using a cell-site simulator to derive a cellphone's location based on involuntarily conveyed signals, "the Government cuts out the middleman and obtains the information directly."[123] Put more succinctly, "[w]ithout a third party, the third party doctrine is inapplicable."[124]

Ultimately, the district court rejected the Government's argument that the warrantless use of the cell-site simulator to locate Lambis was reasonable within the meaning of the Fourth Amendment.[125] The court suppressed the evidence recovered by the DEA agents from Lambis's apartment and quashed the Government's case while warning, "[a]bsent a search warrant, the Government may not turn a citizen's cell phone into a tracking device."[126]

V. Analysis

Amid growing cries to constrain the government's use of electronic surveillance, *United States v. Lambis* serves as a shining example of what courts across the country can do to better safeguard the protections guaranteed by the Fourth Amendment while balancing the needs of law enforcement to control crime.[127] Marking the first federal ruling of its kind[128]—namely that the warrantless use of cell-site simulators constitutes an unreasonable search within the meaning of the Fourth Amendment—the Southern District of New York's elegant analysis in *Lambis* provides other

120. *Lambis*, 197 F. Supp. 3d at 615.

121. *Id.* (citations omitted).

122. *Id.* at 616 (quoting *In re* United States for Historical Cell Site Data, 724 F.3d 600, 610 (5th Cir. 2013)).

123. *Id.*

124. *Id.*

125. *Id.*

126. *Id.* at 611, 616.

127. *See generally id.* at 608-16.

128. Cyrus Farivar, *For the First Time, Federal Judge Tosses Evidence Obtained Via Stingray*, LAW & DISORDER (Sept. 12, 2016, 8:07 PM), https://arstechnica.com/tech-policy/2016/07/for-the-first-time-federal-judge-tosses-evidence-obtained-via-stingray/.

courts with a blueprint to construct similar safeguards and strike a careful balance.[129]

The genius of the *Lambis* opinion stems from the court's willingness to borrow a straight flush from the deck of Fourth Amendment jurisprudence instead of merely playing its ace. For example, the issue of whether cell-site simulators are devices commonly available to the public is certainly a dispositive one.[130] If the district court had solely made findings that cell-site simulators are not devices commonly available to the public, then a warrantless search via a cell-site simulator is theoretically a search that is presumptively unreasonable. An opinion resting on those findings alone, however, would be a dangerous one. If tomorrow the makers of Candy Crush Saga were to release a new iPhone application, "Cell-site Simulator Saga," the district court's reasoning would be swiftly undermined. By using each Fourth Amendment tool at its disposal, the district court built a sturdy opinion with a strong foundation in case law.

The benefit of such an approach is that it makes the district court's analysis easily transferrable to similar cases, even those that may be factually dissimilar. Was your client outside his home at the time law enforcement used a cell-site simulator to pinpoint his location? Try the district court's line of reasoning regarding the third party doctrine.[131] Did the trial court make findings against your client that he voluntarily conveyed his location information to his cellphone service provider and therefore the third party doctrine was triggered? Consider arguing that the government's conduct was unreasonable under the district court's interpretation of *Karo*.[132] If other courts were to adopt an analysis similar to *Lambis*, Fourth Amendment protections would clearly be the winner.[133]

At a time when society is struggling to strike a balance between the legitimate goals of law enforcement and privacy protections, *Lambis* demonstrates how to best address both concerns.[134] Largely unknown to the public until recently, cell-site simulators play an increasing role in law

129. *See* 197 F. Supp. 3d at 608-16.

130. Kyllo v. United States, 533 U.S. 27, 34 (2001) ("[O]btaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area' . . . constitutes a search—at least where . . . the technology in question is not in general public use." (quoting Silverman v. United States, 365 U.S. 505, 512 (1961))).

131. *Lambis*, 197 F. Supp. 3d at 614-16.

132. *Id.* at 611.

133. *See generally id.* at 608-16.

134. *Id.*

enforcement.[135] While the public has become savvy of the government's growing reliance on electronic surveillance and several states have passed legislative restrictions, courts should actively seek to adjudicate claims related to cell-site simulators in a fashion similar to that employed by the Southern District of New York, allowing law enforcement to rely on cell-site simulators only when prior judicial authorization is sought.[136] The government's unfettered power to assemble data so intimately connected with a person's everyday life through real-time location tracking via their cellphone would otherwise certainly have a chilling effect on personal and associational freedoms; indeed, this effect may be so severe as to "alter the relationship between citizen and government in a way that is inimical to democratic society."[137]

VI. Conclusion

John Perry Barlow—a former Wyoming rancher, Grateful Dead lyricist and co-founder of the Electronic Frontier Foundation[138]—once cheekily observed: "Relying on the government to protect your privacy is like asking

135. James B. Astrachan & Christopher J. Lyon, *Cell-Site Simulators and the Fourth Amendment: Government Surveillance*, LEXIS PRAC. ADVISOR J. (2016), https://www.lexisnexis.com/lexis-practice-advisor/the-journal/b/lpa/archive/2016/11/08/cell-site-simulators-and-the-fourth-amendment-government-surveillance.aspx. "[I]nformation about [cell-site simulators] has been difficult to obtain because the government and its contractors have employed non-disclosure agreements to make it difficult for the public to learn of even the mere existence of the devices." *Id.* For example, "the FBI . . . required both the [Baltimore Police Department] and the Office of the State's Attorney for Baltimore City to sign a non-disclosure agreement" as a condition of use. *Id.*

136. *E.g.*, 725 ILL. COMP. STAT. 137 (2017) (prohibiting the use of cell-site simulators without a warrant); 12 R.I. GEN. LAWS § 12-32-2 (2016) (requiring a warrant to obtain location information from a cellphone); VA. CODE ANN. § 19.2-70.3 (2016) (instructing that real-time location data may only be obtained pursuant to a subpoena, a search warrant, a court order, or consumer consent); WASH. REV. CODE. § 9.73.260 (2015) (requiring a prior court order in order to use a cell-site simulator); WIS. STAT. § 968.373 (2015) (mandating that law enforcement must obtain a warrant to track or identify the location of a communication device).

137. United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).

138. *Board of Directors*, ELECTRONIC FRONTIER FOUND., (last visited Mar. 26, 2017), https://www.eff.org/about/board.

a Peeping Tom to install your window blinds."[139] Courts should be wary of the government's intention to use citizens' cellphones as tracking devices without first seeking judicial authorization as cell-site simulators make their way into law enforcement agencies across the country.[140] Even though the purchase and use of cell-site simulators is shrouded in secrecy by many agencies, the American Civil Liberties Union has identified seventy-two federal agencies ranging from the United States Navy to the Internal Revenue Service known to have the technology.[141] Even then, this figure does not include the dozens of state and city agencies (such as the Oklahoma City Police Department) that also have cell-site simulators in their electronic surveillance arsenal.[142] Cell-site simulators, quite literally, are coming to a city near you. As such, courts across the country should heed the command of the Southern District of New York in *United States v. Lambis:* "[T]he Government may not turn a citizen's cell phone into a tracking device."[143]

Kathryn E. Gardner

139. Frank Verbruggen, *The Glass May Be Half-Full or Half-Empty, But It Is Definitely Fragile*, *in* PRIVACY & THE CRIMINAL LAW 121 (Erik Claes, Antony Duff & Serge Gutwirth eds., 2006).

140. *Stingray Tracking Devices: Who's Got Them?*, AM. CIV. LIBERTIES UNION (last visited Mar. 26, 2017), https://www.aclu.org/map/stingray-tracking-devices-whos-got-them.

141. *Id.*

142. *Id.*; Clifton Adcock, *Okla. Authorities Have or Use Controversial Cellphone Tracker*, OKLA. WATCH (last visited Feb. 7, 2017), http://oklahomawatch.org/2016/04/10/okla-authorities-have-or-use-controversial-cell-phone-tracker/.

143. United States v. Lambis, 197 F. Supp. 3d 606, 611 (S.D.N.Y. 2016).