




4-27-2020

## Limited Privacy in “Pings:” Why Law Enforcement’s Use of Cell-Site Simulators Does Not Categorically Violate the Fourth Amendment

Lara M. McMahon

Washington and Lee University School of Law, [mcmahon.l@law.wlu.edu](mailto:mcmahon.l@law.wlu.edu)

Follow this and additional works at: <https://scholarlycommons.law.wlu.edu/wlulr>

 Part of the [Communications Law Commons](#), [Constitutional Law Commons](#), [Criminal Law Commons](#), [Criminal Procedure Commons](#), [Fourth Amendment Commons](#), and the [Science and Technology Law Commons](#)

### Recommended Citation

Lara M. McMahon, *Limited Privacy in “Pings:” Why Law Enforcement’s Use of Cell-Site Simulators Does Not Categorically Violate the Fourth Amendment*, 77 Wash. & Lee L. Rev. 981 (2020).

Available at: <https://scholarlycommons.law.wlu.edu/wlulr/vol77/iss2/9>

This Note is brought to you for free and open access by the Washington and Lee Law Review at Washington and Lee University School of Law Scholarly Commons. It has been accepted for inclusion in Washington and Lee Law Review by an authorized editor of Washington and Lee University School of Law Scholarly Commons. For more information, please contact [christensena@wlu.edu](mailto:christensena@wlu.edu).

# Limited Privacy in “Pings:” Why Law Enforcement’s Use of Cell-Site Simulators Does Not Categorically Violate the Fourth Amendment

Lara M. McMahon\*

## *Table of Contents*

I. Introduction and Background .....	982
A. The Development of Cell-Site Simulators .....	987
B. How Cell-Site Simulators Work .....	988
C. How Law Enforcement Use Cell-Site Simulators ....	990
D. Critiques of Law Enforcement’s Use of Cell-Site Simulators.....	993
II. The Fourth Amendment Governs Law Enforcement’s Use of Cell-Site Simulators .....	994
A. Law Enforcement’s Use of a Cell-Site Simulator Is Not a Fourth Amendment Seizure .....	995
B. Law Enforcement’s Use of a Cell-Site Simulator May Be a Fourth Amendment Search.....	998
1. The Physical Trespass Test.....	1000
2. The <i>Katz</i> Reasonable Expectation of Privacy Test.....	1002
3. Supreme Court Case Law Applying the <i>Katz</i> Test.....	1004
a. <i>United States v. Knotts</i> .....	1004
b. <i>United States v. Karo</i> .....	1007
c. <i>Kyllo v. United States</i> .....	1008

---

\* J.D. Candidate, May 2020, Washington and Lee University School of Law. I would like to thank Professor Timothy C. MacDonnell and my fellow students on the Washington and Lee Law Review for their help and guidance throughout the writing process. Thank you also to my parents—in this, as in all things, I am eternally grateful for your love and support.

d. <i>United States v. Jones</i> .....	1010
e. <i>Carpenter v. United States</i> .....	1012
4. Case Law Applying the <i>Katz</i> Test to Law Enforcement's Use of Cell-Site Simulators .....	1015
a. <i>Maryland v. Andrews</i> .....	1015
b. <i>United States v. Lambis</i> .....	1016
c. <i>Jones v. United States</i> .....	1017
III. Four Factors Courts Should Consider When Analyzing Law Enforcement's Use of a Cell-Site Simulator .....	1020
A. Whether the Surveillance Infringed on a Constitutionally Protected Area .....	1021
B. The Duration of the Surveillance .....	1023
C. Active Versus Passive Surveillance .....	1024
D. The Nature of the Information Obtained by the Surveillance .....	1026
IV. A Search Does Not Violate the Fourth Amendment Unless It Is Unreasonable .....	1029
A. Four Models for Determining Reasonableness .....	1029
B. The Warrant Preference Model Is Best-Suited to Analyzing the Reasonableness of Cell-Site Simulators .....	1031
V. Conclusion .....	1033

### *I. Introduction and Background*

Consider this: an unmarked police vehicle is parked near the intersection of 177th Street and Broadway in the Washington Heights neighborhood of New York City.<sup>1</sup> The police officers inside the vehicle are surveilling a large apartment complex. The officers are investigating an international drug trafficking organization, and they believe their suspect is in one of the apartments in the nearby area. The officers do not know which apartment building, let alone which apartment, belongs to their suspect. Rather than

---

1. This hypothetical is based on the facts underlying *United States v. Lambis*. See *United States v. Lambis*, 197 F. Supp. 3d 606, 609 (S.D.N.Y. 2016) (detailing the process by which DEA agents used a cell-site simulator to locate Raymond Lambis's apartment).

knocking on each of the apartment doors, and without first obtaining a search warrant, the officers deploy a cell-site simulator.<sup>2</sup> The suspect’s phone transmits the cell phone’s serial number and the phone’s location within the apartment complex to the cell-site simulator. Having pinpointed their suspect’s location, the officers proceed to 701 West 177th Street, Apartment 55.<sup>3</sup> The suspect’s father opens the door and gives the officers consent to enter the apartment. The officers arrest the suspect after seeing cocaine on the suspect’s bedside table.

Now, consider this: police officers are investigating a string of sexual assaults in the Washington, D.C. metro area.<sup>4</sup> An unmarked police vehicle is parked just outside the Minnesota Avenue Metro Station. In search of their suspect, the officers inside the vehicle deploy a cell-site simulator, again, without first obtaining a warrant. The suspect’s phone connects with the cell-site simulator, and the cell-site simulator directs the officers to the suspect’s car, which is parked on the side of the street. The suspect and his girlfriend are sitting in the car. After obtaining the suspect’s consent, the officers search the suspect’s car and his person. Upon discovery of one of the victim’s cell phones, the officers arrest the suspect.

The question raised by both of these scenarios is whether the officers violated the individual suspects’ Fourth Amendment rights when the officers deployed cell-site simulators to locate their suspects without first obtaining a search warrant. This Note seeks to answer this question by examining the constitutionality of law enforcement’s use of cell-site simulators, specifically addressing whether the use of a cell-site simulator constitutes a Fourth Amendment search or seizure. This issue is particularly relevant in light of the

---

2. See *infra* Parts I.B and I.C (explaining how cell-site simulators function and how law enforcement officers use them as surveillance tools).

3. Complaint at 2, *United States v. Lambis*, 197 F. Supp. 3d 606 (S.D.N.Y. 2016) (No. 15-CR-00734), 2015 WL 13694512.

4. This hypothetical is based on the facts underlying *Jones v. United States*. See *Jones v. United States*, 168 A.3d 703, 708–09 (D.C. Ct. App. 2017) (describing police officers’ use of a cell-site simulator to locate Prince Jones).

Supreme Court's decision in *Carpenter v. United States*,<sup>5</sup> in which the Court held that law enforcement officers must obtain a search warrant supported by probable cause prior to accessing historic cell-site location information (CSLI).<sup>6</sup>

Although the Supreme Court has never ruled specifically on the issue of cell-site simulators, a number of lower courts have held that law enforcement's use of a cell-site simulator constitutes a Fourth Amendment search.<sup>7</sup> For example, the court in *Maryland v. Andrews*<sup>8</sup> held that Baltimore Police Department officers' warrantless use of a cell-site simulator to track a suspect to an acquaintance's private residence violated the suspect's Fourth Amendment rights because "people have an objectively reasonable expectation of privacy in real-time cell phone location information."<sup>9</sup> Similarly, the court in *Jones v. United States*<sup>10</sup> held that D.C. Metropolitan Police Department officers' "use of a cell-site simulator to locate Mr. Jones's phone" in Jones's car, which was parked on a public street, "invaded a reasonable expectation of privacy and was thus a search."<sup>11</sup> The court in *United States v. Lambis*<sup>12</sup> adopted a somewhat different approach in relying on the

5. 138 S. Ct. 2206 (2018).

6. See *id.* at 2221 ("Having found that the acquisition of Carpenter's CSLI was a search, we also conclude that the Government must generally obtain a warrant supported by probable cause before acquiring such records.").

7. See *Jones*, 168 A.3d at 713 (concluding "that the use of a cell-site simulator to locate Mr. Jones's phone invaded a reasonable expectation of privacy and was thus a search"); *Lambis*, 197 F. Supp. 3d at 611 (concluding that "[t]he use of a cell-site simulator constitute[d] a Fourth Amendment search within the contemplation of *Kyllo*" and that "[a]bsent a search warrant, the Government may not turn a citizen's cell phone into a tracking device"); *Maryland v. Andrews*, 134 A.3d 324, 350 (Ct. Spec. App. Md. 2016) (holding that law enforcement's use of a cell-site simulator requires a search warrant based on probable cause).

8. 134 A.3d 324 (Ct. Spec. App. Md. 2016).

9. *Id.* at 327.

10. 168 A.3d 703 (D.C. Ct. App. 2017). In order to avoid confusion with *United States v. Jones*, 565 U.S. 400 (2012), which is discussed later in this Note, *Jones v. United States* will hereinafter be referred to as "*Jones (D.C.)*".

11. *Jones (D.C.)*, 168 A.3d at 714.

12. 197 F. Supp. 3d 606 (S.D.N.Y. 2016).

Supreme Court’s decision in *Kyllo v. United States*.<sup>13</sup> The *Lambis* court held that DEA agents’ use of a cell-site simulator to track a suspect to his own apartment “was an unreasonable search because the ‘pings’ from Lambis’s cell phone to the nearest cell site were not readily available ‘to anyone who wanted to look’ without the use of a cell-site simulator.”<sup>14</sup> Although *Lambis* can be reconciled with Supreme Court jurisprudence,<sup>15</sup> this Note argues that law enforcement’s warrantless use of cell-site simulators does not, as a general rule, amount to a Fourth Amendment search.

This Note proposes four factors courts should consider when asked to determine whether law enforcement’s use of a cell-site simulator constituted a Fourth Amendment search. The first asks courts to consider whether the cell-site simulator surveillance infringed on a constitutionally protected area, such as the home. The second asks courts to consider the duration of the cell-site simulator surveillance. The third asks courts to consider whether the cell-site simulator surveillance was conducted actively or passively. The fourth asks courts to focus on the nature and depth of the information obtained as a result of the cell-site simulator surveillance. If, after analyzing these four factors, a court concludes that law enforcement officers conducted a Fourth Amendment search, the court must then ask whether the search was reasonable.<sup>16</sup> Cell-site simulators are generally used in the “enterprise of ferreting out crime.”<sup>17</sup> Thus, if law enforcement’s use of a cell-site simulator amounts to a Fourth Amendment search, that search should be considered unreasonable, and therefore

---

13. 533 U.S. 27 (2001).

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

15. See *infra* Part III (critiquing the holdings in *Andrews*, *Lambis*, and *Jones (D.C.)*).

16. See, e.g., *New Jersey v. T.L.O.*, 469 U.S. 325, 340 (1985) (defining the reasonableness requirement as the ultimate touchstone and “fundamental command” of the Fourth Amendment).

17. See *Johnson v. United States*, 333 U.S. 10, 14 (1948) (explaining that a “neutral and detached magistrate,” rather than an officer engaged in the “enterprise of ferreting out crime,” should be the one to determine “[w]hen the right of privacy must reasonably yield to the right of search”).

violative of the Fourth Amendment, if it was conducted without a warrant.<sup>18</sup>

The remainder of this Part provides background information regarding the development and use of cell-site simulators at the federal, state, and local levels. Part II lays out a general framework for analyzing Fourth Amendment search and seizure cases. Part II.A concludes that law enforcement's use of a cell-site simulator does not constitute a Fourth Amendment seizure, but Part II.B argues that it may constitute a Fourth Amendment search. Part II.B then delves into Fourth Amendment search case law, chronicling several key Supreme Court decisions that apply both the traditional, physical trespass test<sup>19</sup> and the *Katz* reasonable expectation of privacy test<sup>20</sup> to various electronic surveillance techniques. Part II.B next analyzes the three cell-site simulator cases referenced earlier in this Part—*Maryland v. Andrews*, *United States v. Lambis*, and *Jones v. United States*—and concludes that the courts in *Andrews* and *Jones (D.C.)* came to overly-broad conclusions in holding that law enforcement's use of cell-site simulators categorically violates individuals' expectations of privacy. Part III proposes four factors courts should consider to determine whether, on a case-by-case basis, law enforcement's use of a cell-site simulator constitutes a Fourth Amendment search. Part IV addresses the Fourth Amendment's reasonableness requirement and concludes that the warrant preference model for determining reasonableness is best-suited to cell-site simulators.

---

18. See *infra* Part IV.B (arguing that the warrant preference model is best-suited to cases where law enforcement officers have used cell-site simulators).

19. See *United States v. Jones*, 565 U.S. 400, 406 (2012) (“[F]or most of our history the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas (‘persons, houses, papers, and effects’) it enumerates.”).

20. See *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (proposing that a reasonable expectation of privacy requires a person “exhibit[] an actual (subjective) expectation of privacy [that] society is prepared to recognize as ‘reasonable’”).

*A. The Development of Cell-Site Simulators*

Prior to 2015, a great deal of secrecy surrounded law enforcement’s use of cell-site simulators.<sup>21</sup> In 2015, the Department of Justice and the Department of Homeland Security issued revised policies regarding the use of cell-site simulators,<sup>22</sup> bringing their use out of the shadows and opening law enforcement’s practices up for critique.<sup>23</sup> Both departments’ policies mandate that their respective federal law enforcement agents obtain search warrants prior to using cell-site simulators.<sup>24</sup> Notably, however, neither department

---

21. See Kristi Winner, Note, *From Historical Cell-Site Location Information to IMSI-Catchers: Why Triggerfish Devices Do Not Trigger Fourth Amendment Protection*, 68 CASE W. RES. L. REV. 243, 254–55 (2017) (positing that the nondisclosure agreements between Harris Corporation, the largest manufacturer of cell-site simulators, and law enforcement agencies are the primary reason for the shroud of secrecy surrounding cell-site simulators).

22. See Press Release, Dep’t of Justice, Justice Department Announces Enhanced Policy for Use of Cell-Site Simulators, at 1 (Sept. 3, 2015), <https://perma.cc/L4WF-Z2P9> (last visited Feb. 3, 2020) (emphasizing the importance of cell-site simulator technology to law enforcement and explaining that, to enhance privacy protections, law enforcement must obtain a search warrant supported by probable cause before using a cell-site simulator) (on file with the Washington and Lee Law Review); Memorandum from Dep’t of Homeland Security on Dep’t Policy Regarding the Use of Cell-Site Simulator Technology, at 4 (Oct. 19, 2015), <https://perma.cc/5RGA-BEXV> (PDF) [hereinafter DHS Policy] (“[A]s a matter of policy, law enforcement Components must now obtain a search warrant supported by probable cause and issued pursuant to Rule 41 of the Federal Rules of Criminal Procedure . . .”); see also FED. R. CRIM. P. 41 (discussing searches and seizures).

23. See, e.g., Laura DeGeer, Note, *Cell-Site Simulators: A Call for More Protective Federal Legislation*, 78 U. PITT. L. REV. 351, 352 (2016) (arguing that Congress should draft a bill “enumerating when, how, and by whom a cell site simulator may be used”); Jenna Jonassen, Note, *Stingrays, Triggerfish, and Hailstorms, Oh My! The Fourth Amendment Implications of the Increasing Government Use of Cell-Site Simulators*, 33 TOURO L. REV. 1123, 1127 (2017) (“[T]his Note attempts to provide an accurate road map of the various types of information concerning cell-site simulator use and how its implications on Fourth Amendment rights call for the establishment of a sufficient probable cause warrant prior to its use.”).

24. See U.S. DEPT OF JUSTICE, DEPARTMENT OF JUSTICE POLICY GUIDANCE: USE OF CELL-SITE SIMULATOR TECHNOLOGY 3 (Sept. 3, 2015), <https://perma.cc/5YYW-D7DY> (PDF) [hereinafter DOJ Policy] (explaining that, before using cell-site simulators, “law enforcement agencies must now



has conceded that law enforcement officers are constitutionally required to obtain a search warrant before using a cell-site simulator.<sup>25</sup> Many state and local law enforcement agencies are not governed by similar policies or state laws and therefore are not required to obtain search warrants before using cell-site simulators.<sup>26</sup> Thus, the constitutionality of law enforcement's use of cell-site simulators remains unclear in many jurisdictions.

### *B. How Cell-Site Simulators Work*

Some familiarity with cell phone technology is necessary to understand the potential Fourth Amendment issues raised by cell-site simulators.<sup>27</sup> A cell phone is essentially a “two-way radio with a low-power transmitter that operates in a network of cell sites.”<sup>28</sup> A “cell” is an area of geographic coverage, often illustrated as a hexagon.<sup>29</sup> A “cell site” is the physical location

---

obtain a search warrant supported by probable cause and issued pursuant to Rule 41 of the Federal Rules of Criminal Procedure”); DHS Policy, *supra* note 22, at 2 (explaining that, before using cell-site simulators, “law enforcement Components must now obtain a search warrant supported by probable cause and issued pursuant to Rule 41 of the Federal Rules of Criminal Procedure”).

25. See, e.g., *United States v. Patrick*, 842 F.3d 540, 545 (7th Cir. 2016) (“The Department of Justice announced last September that in the future it would ordinarily seek a warrant, plus an order under the pen-register statute . . . before using a cell-site simulator, but it has not conceded that this is constitutionally required.”).

26. See *Winner*, *supra* note 21, at 261 nn.136–41 (listing Colorado, Illinois, Indiana, Maine, Maryland, Montana, Tennessee, and Wisconsin as the only states that have enacted statutes that regulate the use of cell-site simulators, and California, Minnesota, Utah, Virginia, and Washington as the only states that have enacted statutes explicitly requiring search warrants to use cell-site simulators); see also *Stingray Tracking Devices: Who’s Got Them?*, ACLU (last updated Nov. 2018), <https://perma.cc/E8LG-AU2J> (last visited Feb. 3, 2020) (mapping law enforcement’s use of cell-site simulators at the federal, state, and local levels) (on file with the Washington and Lee Law Review).

27. See *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 396 F. Supp. 2d 747, 750 (S.D. Tex. 2005) (beginning the discussion of prospective cell-site data with an overview of basic cell phone technology).

28. *Id.*

29. *Id.*

where the radio transceiver and base station controller are located.<sup>30</sup> Cell sites send and receive traffic from cell phones in their geographic areas to switching offices, which handle the phone connections and controls for a given region.<sup>31</sup> Most modern cell phones connect with cell sites several times per minute.<sup>32</sup> Cell phones are constantly scanning their environments for the strongest signal, even when they are not in use.<sup>33</sup> Generally, the strongest cell phone signal comes from the closest cell site.<sup>34</sup>

When activated, a cell-site simulator mimics legitimate cell sites by sending out broadcasts to cell phones in its vicinity.<sup>35</sup> Nearby cell phones then identify the cell-site simulator as the closest, most attractive cell site in the area, connecting with the cell-site simulator instead of a legitimate

---

30. *Id.*

31. *Id.*

32. *See id.* (“The cell phone re-scans every seven seconds or when the signal strength weakens, regardless of whether a call is placed.”); *Carpenter v. United States*, 138 S. Ct. 2206, 2211 (2018) (explaining that cell phones connect with their wireless networks even when the owner is not using one of the cell phone’s features).

33. *See id.* (“When a cell phone is powered up, it acts as a scanning radio, searching through a list of control channels for the strongest signal.”).

34. *See id.* (“Cell phones continuously scan their environment looking for the best signal, which generally comes from the closest cell site.”).

35. *See* Orin Kerr, *Applying the Fourth Amendment to Cell-Site Simulators*, WASH. POST (Apr. 4, 2016), <https://perma.cc/EA8B-Z6C4> (last visited Feb. 3, 2020) (“The simulators send out broadcasts to phones in the neighborhood just as a real cell site would.”) (on file with the Washington and Lee Law Review); *Cell Site Simulators, A National Association of Criminal Defense Lawyers Primer*, BERKELEY TECH. & PUB. POL’Y CLINIC (Apr. 28, 2016), <https://perma.cc/MV3F-3VQW> (PDF) [hereinafter NACDL Primer] (providing an overview of how cell-site simulators work and outlining ways for defense lawyers to challenge the admissibility of evidence obtained via cell-site simulators); *Cell-Site Simulators/IMSI Catchers*, ELECTRONIC FRONTIER FOUND., <https://perma.cc/92NJ-44XJ> (last visited Feb. 3, 2020) (describing cell-site simulators as “devices that masquerade as legitimate cell phone towers, tricking phones within a certain radius into connecting to the device rather than a tower”) (on file with the Washington and Lee Law Review); C. Justin Brown & Kasha M. Leese, *StingRay Devices Usher in a New Fourth Amendment Battleground*, CHAMPION, June 2015, at 13 (reporting that a cell-site simulator is a device that can “locate the source of a cellular signal without going through the wireless carrier”).

cell site.<sup>36</sup> Cell phones have no way of distinguishing between legitimate cell sites and cell-site simulators.<sup>37</sup>

### C. How Law Enforcement Use Cell-Site Simulators

Once a cell-site simulator has connected with a cell phone, law enforcement officers can identify the direction and signal strength of that particular cell phone.<sup>38</sup> By shifting the location of the cell-site simulator, an officer can determine the cell phone's location more precisely than if she were to triangulate the cell phone's signal using its CSLI.<sup>39</sup> Due to their relatively small size, officers can either carry cell-site simulators by hand or deploy them in vehicles for larger-scale surveillance.<sup>40</sup>

---

36. See DOJ Policy, *supra* note 24, at 2 (“In response to the signals emitted by the simulator, cellular devices . . . identify the simulator as the most attractive cell tower in the area and thus transmit signals to the simulator that identify the device in the same way that they would with a networked tower.”).

37. See Stephanie K. Pell & Christopher Soghoian, *Your Secret StingRay's No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy*, 28 HARV. J.L. & TECH. 1, 12 (“As a result [of cell phones’ inability to authenticate cell sites], phones have no way to differentiate between a legitimate base station owned or operated by the target’s wireless carrier and a rogue device impersonating a carrier’s base station.”).

38. See Brown & Leese, *supra* note 35, at 13–14 (summarizing the additional equipment needed to operate a cell-site simulator, which includes “an antenna, a device that processes the signals transmitted on cell phone frequencies, and a laptop computer that analyzes the signals and allows the agent to configure the incoming information”).

39. See *id.* at 14 (distinguishing cell-site simulators from cell tower tracking: “cell site simulators produce extremely precise location information, in some cases within an accuracy of approximately six feet”).

40. See NACDL Primer, *supra* note 35, at 1 (describing cell-site simulators as “portable, briefcase-sized devices, which can fit in small cars, be carried by hand, and even be deployed on airplanes to facilitate larger-scale surveillance”); see also Kim Zetter, *California Police Used Stingrays in Planes to Spy on Phones*, WIRED (Jan. 1, 2017), <https://perma.cc/MQ8K-GYHB> (last visited Feb. 3, 2020) (recounting the Anaheim Police Department’s use of Dirtboxes, or plane-mounted cell-site simulators, to conduct surveillance above Disneyland) (on file with the Washington and Lee Law Review).

Law enforcement officers can also use cell-site simulators to obtain a cell phone’s identifying information,<sup>41</sup> including its international mobile subscriber number, mobile identification number, and electronic serial number.<sup>42</sup> Once a cell-site simulator has connected with a cell phone, the cell-site simulator will obtain the signaling information relating only to that particular device.<sup>43</sup>

Depending on the jurisdiction, law enforcement officers may have access to both passive and active cell-site simulators.<sup>44</sup> Passive cell-site simulators intercept the signals sent between nearby cell phones and cell sites, but do not transmit any signals of their own.<sup>45</sup> As a result, passive cell-site simulators “can only detect signals of nearby phones when those phones are actually transmitting data.”<sup>46</sup> Active cell-site simulators, as the name suggests, directly interact

---

41. “Identifying information” includes the International Mobile Equipment Identity (IMEI), a unique number assigned to each handset, and the International Mobile Subscriber Identity (IMSI), a unique number assigned to each SIM card. *See* NACDL Primer, *supra* note 35, at 1.

42. *See* Brown & Leese, *supra* note 35, at 13 n.9 (“IMSI is the acronym for ‘[i]nternational mobile subscriber identity,’ which is a cellphone’s unique identifier.”); DEPT’ OF JUSTICE, ELECTRONIC SURVEILLANCE MANUAL PROCEDURES AND CASE LAW FORMS 40 (June 2005), <https://perma.cc/2KEU-6B5W> (PDF) [hereinafter DOJ SURVEILLANCE MANUAL] (explaining that an MIN is a cell phone’s telephone number, while an ESN is the number assigned by the cell phone’s manufacturer to the cell phone); *see also* *Cell-Site Simulators/IMSI Catchers*, *supra* note 35 (“Once your cellular device has connected to a cell-site simulator, the cell-site simulator can determine your location and read identifying data such as IMSI or ESN numbers directly from your mobile device.”).

43. *See* DHS Policy, *supra* note 22, at 3 (explaining that “[c]ell-site simulators provide only the relative signal strength and general direction of the subject cellular device; they do not function as a OPS locator, as they do not obtain or download any location information from the device or its applications”).

44. *See* Pell & Soghoian, *supra* note 37, at 9 (“The technologies that enable the direct interception of cellular phone calls without the assistance of a wireless carrier generally fall into two categories: *passive* and *active*.”).

45. *Id.*

46. *See id.* at 12 (noting that one advantage of passive cell-site simulators is that they are “far more covert in operation—indeed effectively invisible”).

with the cell phones they are used to surveil.<sup>47</sup> An active cell-site simulator impersonates a cell-site by sending out broadcasts to phones in its vicinity.<sup>48</sup> Thus, active cell-site simulators can connect with cell phones that are not in use.<sup>49</sup>

Law enforcement's use of cell-site simulators is distinguishable from cell tower tracking, or the use of CSLI to triangulate a cell phone's signal.<sup>50</sup> However, law enforcement officers often use cell-site simulators in tandem with CSLI.<sup>51</sup> CSLI is the time-stamped record generated by a cell phone each time it connects with a cell site.<sup>52</sup> Wireless carriers collect and store CSLI for their own business purposes,<sup>53</sup> often for years at a time.<sup>54</sup> Law enforcement officers use CSLI to determine a cell phone's approximate location, either

---

47. *Id.*

48. *See* Kerr, *supra* note 35 (“The simulators send out broadcasts to phones in the neighborhood just as a real cell site would.”).

49. *See* Pell & Soghoian, *supra* note 37, at 13 (noting that, unlike their passive counterparts, active cell-site simulators can “rapidly identify and locate all nearby phones that are turned on, even if they are not transmitting any data”).

50. *See* Stephanie Lacambra, *Cell Phone Location Tracking or CSLI: A Guide for Criminal Defense Attorneys*, ELECTRONIC FRONTIER FOUND. 1, <https://perma.cc/WN9C-M7JP> (PDF) (discussing ways in which criminal defense attorneys can challenge the admissibility of cell phone location data).

51. *See* United States v. Lambis, 197 F. Supp. 3d 606, 609 (S.D.N.Y. 2016) (“Using CSLI, DEA agents were able to determine that the target cell phone was located in the general vicinity of ‘the Washington Heights area by 177th and Broadway.’” (citation omitted)).

52. *See* Carpenter v. United States, 138 S. Ct. 2206, 2211–12 (2018) (explaining that cell phones function by continuously connecting to a set of radio antennas, or cell sites, and that each time a cell phone connects to a cell site, it generates a time-stamped record); *Lambis*, 197 F. Supp. 3d at 608–09 (describing CSLI as “a record of non-content-based location information from the service provider derived from ‘pings’ sent to cell sites by a target cell phone”).

53. *See* Carpenter, 138 S. Ct. at 2212 (listing the following business purposes for retaining CSLI: finding weak spots in networks, applying “roaming” charges, and selling aggregated location records to data brokers).

54. *See* Susan Freiwald & Stephen Wm. Smith, *The Carpenter Chronicle: A Near Perfect Surveillance*, 132 HARV. L. REV. 205, 213 (2018) (discussing telecom companies' move toward retaining CSLI for periods of a year or more as they realized the “potential for huge profits by monetizing such location data”).

historically<sup>55</sup> or in real-time.<sup>56</sup> The precision of the determination depends on the number of cell sites in the area and can range from “a few blocks to several square miles.”<sup>57</sup>

#### *D. Critiques of Law Enforcement’s Use of Cell-Site Simulators*

Privacy advocates such as the Electronic Frontier Foundation (EFF) and the American Civil Liberties Union (ACLU) have argued that law enforcement’s use of cell-site simulators raises a number of privacy concerns.<sup>58</sup> One such argument is that when law enforcement use a cell-site simulator to ascertain the location of a target cell phone, they invade the target cell phone user’s expectations of privacy in her physical location and thus violate the Fourth

---

55. See NACDL Primer, *supra* note 35, at 1 n.6 (“Call detail records include the following information in relation to a phone call: time, duration, historical cell phone location information, completion status, source number, and destination number.”); see also *Carpenter*, 138 S. Ct. at 2213 (describing how, by using Carpenter’s CSLI, an FBI agent was able to produce a map retroactively placing Carpenter’s cell phone near the locations of four robberies).

56. See Lacambra, *supra* note 50, at 1 (noting that cell phone companies also store prospective data, which allows law enforcement officers to track a cell phone’s movements in real-time); NACDL Primer, *supra* note 35, at 1 (“Prospective location information, on the other hand, helps law enforcement trace the current whereabouts of a suspect, which can lead to arrest.”); *United States v. Skinner*, 690 F.3d 772, 776 (6th Cir. 2012) (describing law enforcement’s use of prospective CSLI to apprehend a suspect).

57. See NACDL Primer, *supra* note 35, at 1 n.2; see also *Carpenter*, 138 S. Ct. at 2211–12 (2018) (observing that wireless carriers’ installation of more cell sites has led to increasingly compact coverage areas in urban areas).

58. See, e.g., *Cell Site Simulators/IMSI Catchers*, *supra* note 35 (maintaining that cell-site simulators disrupt cell phone communications); Brown & Leese, *supra* note 35, at 15 (arguing that the “invasive action” law enforcement officers engage in when they use cell-site simulators “is akin to a police officer scrolling through a phone’s records”); Memorandum from the Am. Civil Liberties Union on Fed. Recommendations on the Use of Cell-Site Simulators, at 1, <https://perma.cc/25M8-AYQG> (PDF) (“Policies governing the use of these devices fail to comply with the Fourth Amendment, raise significant civil liberties and privacy concerns, and undermine effective judicial and Congressional oversight.”).

Amendment.<sup>59</sup> Privacy advocates have also raised concerns regarding cell-site simulators' ability to connect with large swaths of cell phone users at any given time,<sup>60</sup> arguing that such use of cell-site simulators allows law enforcement to engage in dragnet surveillance.<sup>61</sup> This Note only seeks to address the first method of surveillance—law enforcement's use of cell-site simulators to track a target cell phone user.

## *II. The Fourth Amendment Governs Law Enforcement's Use of Cell-Site Simulators*

The Fourth Amendment protects “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures”<sup>62</sup> and “to secure the ‘privacies of life’ against ‘arbitrary power.’”<sup>63</sup> The terms

---

59. See *How to Challenge the Use of Cell-Site Simulators*, ELECTRONIC FRONTIER FOUND., <https://perma.cc/X98N-QR9D> (last visited Feb. 3, 2020) (providing examples of arguments defense attorneys can use in challenging law enforcement's use of cell-site simulators) (on file with the Washington and Lee Law Review); Letter from Nathan Freed Wilder, Am. Civil Liberties Union, to John Brooks, Chief of Police, Sunrise, Florida (Feb. 28, 2014), <https://perma.cc/P7SV-KBYX> (PDF) [hereinafter ACLU Letter] (“And using a cell site simulator to ascertain the location of a specific cell phone can reveal that it is in a constitutionally protected place, such as a home, that has traditionally been immune from search unless law enforcement agents obtain a warrant based on probable cause.”).

60. See Zetter, *supra* note 40, at 2 (“Stingrays don’t just pick up the IDs of targeted devices, however. Every phone within range will contact the system, revealing their ID.”).

61. See *Cell-Site Simulators/IMSI Catchers*, *supra* note 35 (arguing cell-site simulators facilitate “indiscriminate, dragnet searches” of “phones located in traditionally protected private spaces, such as homes and doctors’ offices”); Freiwald & Smith, *supra* note 54, at 229 (arguing that “this is also an easy case to predict” because the use of cell-site simulators “raises the specter of an illegal general warrant”); ACLU Letter, *supra* note 59 (“Collecting unique identifiers of all phones in a particular location inherently collects location data on many innocent people.”).

62. U.S. CONST. amend. IV.

63. See *Carpenter v. United States*, 138 S. Ct. 2206, 2214 (2018) (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)); see also *Camara v. Mun. Court of S.F.*, 387 U.S. 523, 528 (1967) (describing the basic purpose of the Fourth Amendment as “safeguard[ing] the privacy and security of individuals against arbitrary invasions by the government”); *United States v. Di Re*, 332 U.S. 581, 595 (1948) (noting that one of the Framers’ central

“search” and “seizure” are terms of limitation.<sup>64</sup> As such, “[l]aw enforcement practices are not required by the Fourth Amendment to be reasonable unless they are either ‘searches’ or ‘seizures.’”<sup>65</sup> To qualify as a search or seizure, law enforcement practices must “bear the requisite relationship to ‘persons, houses, papers, and effects.’”<sup>66</sup> Accordingly, in examining the constitutionality of cell-site simulators, a threshold question that must be answered is whether law enforcement’s use of a cell-site simulator is a search or seizure that infringes on individuals’ rights to be secure in their persons, houses, papers, and effects.<sup>67</sup>

*A. Law Enforcement’s Use of a Cell-Site Simulator Is Not a Fourth Amendment Seizure*

A “seizure’ of property occurs when there is some meaningful interference with an individual’s possessory interests in that property.”<sup>68</sup> Case law regarding law enforcement’s use of electronic tracking devices is particularly

---

aims in drafting the Fourth Amendment was “to place obstacles in the way of a too permeating police power”).

64. WAYNE R. LAFAVE, *SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT* § 2.1 (5th ed. 2019) (citing Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 356 (1974)).

65. *Id.*

66. Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 356 (1974); *see also* Orin Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 540 (2005) (describing the need for “some sort of legitimate relationship between the property searched and the defendant . . . to generate Fourth Amendment rights” where law enforcement searches electronically stored evidence).

67. *See, e.g.*, *Burdeau v. McDowell*, 256 U.S. 465, 475 (1921) (holding that the Fourth Amendment only limits governmental action and does not reach private searches or seizures).

68. *See United States v. Jacobsen*, 466 U.S. 109, 114 (1984) (explaining that the definition of seizure of property follows from the Supreme Court’s oft-repeated definition of the seizure of a person as “meaningful interference, however brief, with an individual’s freedom of movement” (citing *Michigan v. Summers*, 452 U.S. 692, 696 (1981))); Mark Taticchi, Note, *Redefining Possessory Interests: Perfect Copies of Information as Fourth Amendment Seizures*, 78 GEO. WASH. L. REV. 476, 477 (2010) (“Courts generally interpret possessory interest to mean physical possession, even when the property allegedly seized is intangible, like information.”).



helpful in determining whether law enforcement seize a cell phone user's location information when a targeted cell phone connects to a cell-site simulator. In *United States v. Karo*,<sup>69</sup> the Supreme Court addressed "whether installation of a beeper in a container of chemicals with the consent of the original owner constitute[d] a search or seizure within the meaning of the Fourth Amendment when the container is delivered to a buyer having no knowledge of the presence of the beeper."<sup>70</sup> In *Karo*, DEA agents had obtained a court order authorizing the installation and monitoring of a beeper in one of the cans of ether ordered by James Karo.<sup>71</sup> After substituting a can containing a beeper for one of the cans in Karo's shipment, the agents were able to track Karo to his residence, to a storage facility, and eventually, to an accomplice's residence.<sup>72</sup> The Court held that the actual placement of the beeper did not constitute a seizure<sup>73</sup> because the beeper's placement did not interfere with Karo's possessory interest in the can of ether in a "meaningful way."<sup>74</sup> Under the *Karo* Court's reasoning, therefore, a "technical" and "physical" trespass does not constitute a Fourth Amendment seizure if the trespass does not interfere with an individual's possessory interest in a meaningful way.<sup>75</sup>

Law enforcement do not seize a target user's cell phone in violation of the Fourth Amendment when they deploy a cell-site simulator. Although cell-site simulators may interfere

---

69. 468 U.S. 705 (1984).

70. *Id.* at 707.

71. *Id.* at 708.

72. *Id.*

73. *See id.* at 713 ("We conclude that no Fourth Amendment interest of Karo or of any other respondent was infringed by the installation of the beeper. Rather, any impairment of their privacy interests that may have occurred was occasioned by the monitoring of the beeper.").

74. *See id.* at 712 (relying on the traditional definition of "seizure" as some meaningful interference with an individual's possessory interests in the seized property to support the holding that no Fourth Amendment seizure took place).

75. *See id.* at 713 (cautioning that "if the presence of a beeper in the can constituted a seizure merely because of its occupation of space, it would follow that the presence of any object, regardless of its nature, would violate the Fourth Amendment").

“with the functioning’ of, or ‘coopt[ing]’ of [the] phone involved,”<sup>76</sup> such interference is “akin to the interruptions or intrusions [that] . . . are permissible when police officers execute a search incident to arrest that turns up a cell phone.”<sup>77</sup> The cell-site simulator does not, by “[h]old[ing] on to [a cell phone] for a minute,” *meaningfully* interfere with the cell phone user’s possessory interest.<sup>78</sup> Thus, under *Karo*, law enforcement’s use of a cell-site simulator does not amount to a Fourth Amendment seizure.

Writing in dissent in *Karo*, Justice Stevens argued that “the surreptitious use of a radio transmitter . . . on an individual’s personal property is both a seizure and a search within the meaning of the Fourth Amendment.”<sup>79</sup> Justice Stevens relied on a property owner’s right to exclude<sup>80</sup> in concluding that “[w]hen the Government attaches an electronic monitoring device to that property, it infringes that exclusionary right; in a fundamental sense it has converted the property to its own use.”<sup>81</sup> According to Justice Stevens, any interference with an individual’s possessory rights, which include the right to exclude, is a meaningful interference: “[T]he character of the property is profoundly different when infected with an electronic bug than when it is entirely germ free.”<sup>82</sup>

---

76. This interference includes “having . . . calls dropped.” *Jones v. United States*, 168 A.3d 703, 743 n.39 (D.C. Ct. App. 2017).

77. *Id.* (citing *Riley v. California*, 573 U.S. 373, 386–89 (2014)). In the search incident to a lawful arrest context, police officers are “free to examine the physical aspects of [the] phone,” may “turn the phone off or remove its battery,” or may “leave a phone powered on and place it in an enclosure that isolates the phone from radio waves.” *Id.*

78. *Id.* at 743.

79. *See Karo*, 468 U.S. at 728 (Stevens, J., dissenting) (writing to express his belief that “the Fourth Amendment’s reach is somewhat broader than that which is explicitly acknowledged by the Court”).

80. *See Int’l News Serv. v. Associated Press*, 248 U.S. 215, 250 (1918) (Brandeis, J., dissenting) (“An essential element of individual property is the legal right to exclude others from it.”); RESTATEMENT OF PROP. § 7 (AM. LAW INST. 1936) (“A possessory interest in land exists in a person who has . . . an intent so to exercise such control as to exclude other members of society in general from any present occupation of the land.”).

81. *Karo*, 468 U.S. at 728.

82. *Id.* at 729.

Arguably, under Justice Stevens's rationale, the use of a cell-site simulator could be considered a seizure of the target user's cell phone because the cell-site simulator interferes with the user's most fundamental possessory rights.<sup>83</sup> If a cell-site simulator effectively turns an individual's cell phone into a tracking device,<sup>84</sup> the cell phone owner's property has been converted to the government's use, thus violating the cell phone owner's right to exclude.<sup>85</sup> Despite the potential viability of Justice Stevens's dissent in *Karo*, it was not adopted in any of the lower court decisions that have addressed the constitutionality of cell-site simulators.<sup>86</sup>

*B. Law Enforcement's Use of a Cell-Site Simulator May Be a Fourth Amendment Search*

Like the term "seizure," "search" is a term of art in Fourth Amendment jurisprudence.<sup>87</sup> Since the Supreme Court's

---

83. See, e.g., Thomas W. Merrill, *Property and the Right to Exclude*, 77 NEB. L. REV. 730, 730 (1998) (arguing that the right to exclude is "more than just 'one of the most essential' constituents of property—it is the *sine qua non*" (quoting *Kaiser Aetna v. United States*, 444 U.S. 164, 176 (1979))).

84. See *United States v. Lambis*, 197 F. Supp. 3d 606, 611 (S.D.N.Y. 2016) (holding that, "[a]bsent a search warrant, the Government may not turn a citizen's cell phone into a tracking device").

85. See *United States v. Karo*, 468 U.S. 705, 728 (1984) (Stevens, J., dissenting) ("When the Government attaches an electronic monitoring device to that property, it infringes that exclusionary right; in a fundamental sense it has converted the property to its own use."); *Evers v. Cty. of Custer*, 745 F.2d 1196, 1201 (9th Cir. 1984) ("A property owner's right to exclude others is universally held to be a fundamental element of the property right." (citation omitted)).

86. See *Lambis*, 197 F. Supp. 3d at 608 (examining whether *Lambis*'s motion to suppress evidence of "narcotics and drug paraphernalia recovered by law enforcement agents in connection with a search of his apartment" should be granted on the grounds that law enforcement's use of a cell-site simulator constituted a Fourth Amendment search); *State v. Andrews*, 134 A.3d 324, 326 (Md. Ct. Spec. App. 2016) (noting that the case presented "a Fourth Amendment issue of first impression in this State: whether a cell phone—a piece of technology so ubiquitous as to be on the person of practically every citizen—may be transformed into a real-time tracking device by the government without a warrant").

87. See THOMAS K. CLANCY, *THE FOURTH AMENDMENT, ITS HISTORY AND INTERPRETATION* 420 (3d ed. 2017) (noting that while the Supreme Court has occasionally consulted the dictionary and similar sources for their definitions

decision in *Katz v. United States*,<sup>88</sup> both “[e]xpectations of privacy and property interests govern the analysis of Fourth Amendment search . . . claims.”<sup>89</sup> Although the Supreme Court has predominantly relied on the reasonable expectation of privacy test since deciding *Katz* in 1967,<sup>90</sup> the physical trespass test has regained viability<sup>91</sup> in the wake of the Court’s decision in *United States v. Jones*.<sup>92</sup> Accordingly, whether law enforcement’s use of cell-site simulators interferes with individuals’ rights to be secure in their “persons, houses, papers, and effects”<sup>93</sup> must be analyzed under both the *Katz* reasonable expectation of privacy test<sup>94</sup> and the physical trespass test.<sup>95</sup>

---

of “search,” it has not formally adopted those definitions); LAFAVE, *supra* note 64, § 2.1(a)

The meaning of the word “searches,” the matter of primary concern in this Chapter, is not as easily captured within any verbal formulation. Under the traditional approach, the term “search” is said to imply some exploratory investigation, or an invasion and quest, a looking for or seeking out. The quest may be secret, intrusive, or accomplished by force, and it has been held that a search implies some sort of force, either actual or constructive, much or little.

88. 389 U.S. 347 (1967).

89. *United States v. Padilla*, 508 U.S. 77, 82 (1993) (per curiam).

90. *See, e.g.*, CLANCY, *supra* note 87, at 118 (noting that Justice Harlan’s concurring opinion in *Katz* has endured “as the predominant measure for the scope of the Fourth Amendment’s protections”).

91. *See id.* at 103–04 (emphasizing the Supreme Court’s recognition that the Fourth Amendment protects property interests as well as possessory and liberty interests and that the property-based analysis has regained viability since *Katz*); *see also* *United States v. Jones*, 565 U.S. 400, 418 (2012) (concluding that the government’s placement of a GPS tracking device on Jones’s vehicle “supplie[d] a narrower basis for decision” that allowed the Court to decide the case under the physical trespass test).

92. 565 U.S. 400 (2012).

93. U.S. CONST. amend. IV.

94. *See Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (proposing that a reasonable expectation of privacy requires a person “exhibit[] an actual (subjective) expectation of privacy [that] society is prepared to recognize as ‘reasonable’”).

95. *See, e.g.*, *Jones*, 565 U.S. at 405 (explaining that the text of the Fourth Amendment reflects its close connection to property); *Olmstead v. United States*, 277 U.S. 438, 464 (1928) (limiting an individual’s protected interest under the Fourth Amendment to “material things,” such that

### 1. *The Physical Trespass Test*

Fourth Amendment protections were originally grounded in common law property concepts.<sup>96</sup> As a product of the eighteenth century's strong concern for protection of property rights against arbitrary and general government searches,<sup>97</sup> courts have often viewed the Fourth Amendment's historical context as a primary source for understanding the Amendment itself.<sup>98</sup> Under the physical trespass test, which asks whether the government "physically occupied private property for the purpose of obtaining information,"<sup>99</sup> the Fourth Amendment's protections are effectively limited to the physical aspects of "persons, houses, papers, and effects."<sup>100</sup>

Decided in 2012, *United States v. Jones* signaled a revival of the physical trespass test and the end of the *Katz*-dominated era of Supreme Court jurisprudence. Relying on the physical trespass test, the *Jones* Court held 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, constitute[d] a 'search.'"<sup>101</sup> Writing for the majority, Justice Scalia relied on

---

conversations were not protected against unreasonable searches under the Fourth Amendment because they were not included in the list of tangible objects specified in the text of the Fourth Amendment), *overruled by* *Katz v. United States*, 389 U.S. 347 (1967) (concluding that "the underpinnings of *Olmstead* . . . have been so eroded by our subsequent decisions that the 'trespass' doctrine there enunciated can no longer be regarded as controlling").

96. See CLANCY, *supra* note 87, at 9 (describing the Supreme Court's use of property concepts to limit the protections of the Amendment to "persons, places, houses, and effects," thus dividing the world into areas that were constitutionally protected and those that were not).

97. See Thomas K. Clancy, *What Is a 'Search' Within the Meaning of the Fourth Amendment*, 70 ALB. L. REV. 1, 4 (2006) (pointing out that it was the Founders' reaction to the English and colonial search and seizure abuses that culminated in the adoption of the Fourth Amendment).

98. See CLANCY, *supra* note 87, at 104–05 (clarifying the justification for the Framers' inclusion of the notion that "a man's house is his castle" in the Fourth Amendment).

99. *Jones*, 565 U.S. at 404.

100. U.S. CONST. amend. IV.

101. *Jones*, 565 U.S. at 404.

the Fourth Amendment’s “close connection to property.”<sup>102</sup> Justice Scalia emphasized that an individual’s protected interests under the Fourth Amendment do not rise or fall with the *Katz* formulation because, in determining whether a search has taken place, “[a]t bottom, [the Court] must ‘assure[] preservation of that degree of privacy against government intrusion that existed when the Fourth Amendment was adopted.’”<sup>103</sup> Accordingly, the *Jones* Court reaffirmed the proposition that the *Katz* reasonable expectation of privacy test is an addition to, rather than replacement for, the common law trespassory test.<sup>104</sup>

In their separate dissents in *Carpenter v. United States*, Justices Kennedy, Thomas, and Gorsuch signaled a willingness to apply the physical trespass test to determine whether a review of historical CSLI constitutes a Fourth Amendment search.<sup>105</sup> The Justices’ underlying rationales for utilizing the physical trespass test were, however, based largely on the third-party doctrine<sup>106</sup> and thus are inapplicable to the location information obtained via cell-site simulators.

---

102. See *id.* at 405 (“The text of the Fourth Amendment reflects its close connection to property, since otherwise it would have referred simply to ‘the right of the people to be secure against unreasonable searches and seizures’; the phrase ‘in their persons, houses, papers, and effects’ would have been superfluous.”).

103. *Id.* at 406 (quoting *Kyllo v. United States*, 533 U.S. 27, 34 (2001)).

104. See, e.g., *Soldal v. Cook Co.*, 506 U.S. 56, 64 (1992) (explaining that the Fourth Amendment protects individual privacy against certain kinds of governmental intrusion, but its protections go further, and often have nothing to do with privacy at all).

105. See *Carpenter v. United States*, 138 S. Ct. 2206, 2223–24 (2018) (Kennedy, J., dissenting) (advocating for “[a]dherence to this Court’s longstanding precedents and analytic framework,” specifically, to the “property-based concepts that have long grounded the analytic framework that pertains in [Fourth Amendment] cases”); *id.* at 2235 (Thomas, J., dissenting) (arguing that “[t]his case should turn not on ‘whether’ a search occurred,” but on “whose property was searched”); *id.* at 2267 (Gorsuch, J., dissenting) (advocating in favor of a traditional property-based approach in which the Court need only ask whether “a house, paper or effect is yours under law”).

106. See, e.g., *United States v. Miller*, 425 U.S. 435, 440 (1976) (concluding that Miller could not assert ownership or possession over subpoenaed bank records because they were the bank’s business records and not his “private papers”).

Unlike the location information obtained via cell-site simulators, CSLI is physical data that is stored by third-party wireless carriers.<sup>107</sup> The third-party doctrine does not apply to the location information obtained by cell-site simulators because, in using a cell-site simulator, law enforcement officers “cut[] out the middleman and obtain[] the information directly from the targeted cell phone.”<sup>108</sup> When there is no third party, the third-party doctrine is inapplicable.<sup>109</sup> While it is true that “Fourth Amendment rights do not rise or fall with the *Katz* formulation,” because cell-site simulators do not generate physical records stored by third-parties, their use should be analyzed under the *Katz* reasonable expectation of privacy test.<sup>110</sup>

## 2. *The Katz Reasonable Expectation of Privacy Test*

Under the two-pronged *Katz* test, in order to assert an interest protected under the Fourth Amendment, a person must exhibit (1) an actual, subjective expectation of privacy that (2) society is prepared to recognize as reasonable.<sup>111</sup> If

---

107. See Robinson Meyer, *This Very Common Cellphone Surveillance Still Doesn't Require a Warrant*, ATLANTIC (Apr. 14, 2016), <https://perma.cc/R9VT-D7HN> (last visited Feb. 3, 2020).

Right now, CSLI comes in three flavors. The first is “real-time,” where police work with a cell provider to access location data immediately after it’s created. This usually does require a warrant. The second is a “tower dump,” when authorities ask for all the phones that have communicated with a certain tower during a period of time. There’s not a lot of law about how tower dumps work, but as of September of last year cops rarely sought a warrant for them. The third is historical CSLI, where law enforcement requests a backlog of location data created by a certain phone.

(on file with the Washington and Lee Law Review).

108. *United States v. Lambis*, 197 F. Supp. 3d 606, 616 (S.D.N.Y. 2016).

109. See *id.* (“Without a third party, the third-party doctrine is inapplicable.”).

110. *United States v. Jones*, 565 U.S. 400, 406 (2012).

111. See *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (proposing that a reasonable expectation of privacy requires a person “exhibit[] an actual (subjective) expectation of privacy,” and “the expectation be one that society is prepared to recognize as ‘reasonable’”).

either prong is missing, then there is no protected interest, and the Fourth Amendment does not apply.<sup>112</sup> The *Katz* majority, in concluding that law enforcement violated Katz’s reasonable expectation of privacy by placing a recording device outside the public phone booth from which Katz had placed his calls, explained that the Fourth Amendment protects people and not places.<sup>113</sup> After *Katz*, therefore, a Fourth Amendment analysis no longer exclusively “turn[s] upon the presence or absence of a physical intrusion into any given enclosure.”<sup>114</sup>

The first prong of the *Katz* test requires an individual to have exhibited “an actual (subjective) expectation of privacy.”<sup>115</sup> The first prong looks at whether an individual, by her conduct, has shown that she “seeks to preserve [something] as private.”<sup>116</sup> Justice Harlan clarified that analysis under *Katz* “must . . . transcend the search for subjective expectations,” because “[o]ur expectations, and the risks we assume, are in large part reflections of laws that translate into

---

112. See CLANCY, *supra* note 87, at 118 (contrasting Justice Harlan’s two-part test with the *Katz*’s majority opinion, which spoke in terms of unadorned privacy, without modification by any inquiry into subjectivity or reasonableness); see also, e.g., *United States v. Knotts*, 460 U.S. 276, 281 (1983) (holding that the government’s use of a beeper to monitor defendant Petschen’s movements was not a Fourth Amendment search because a “person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another”).

113. See *Katz*, 389 U.S. at 350 (“[T]his effort to decide whether or not a given ‘area,’ viewed in the abstract, is ‘constitutionally protected’ deflects attention from the problem presented by this case. For the Fourth Amendment protects people, not places.”).

114. See *id.* at 353 (“[O]nce it is recognized that the Fourth Amendment protects people—and not simply ‘areas’—against unreasonable searches and seizures it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure.”).

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

116. *Id.* at 351 (majority opinion). Professor Wayne LaFave provides a helpful example of a defendant whose expectation of privacy could not be considered reasonable: “a person openly engaged in criminal conduct in Times Square at high noon, who police observed engaging in criminal conduct.” LAFAVE, *supra* note 64, at § 2.1(c).



rules the customs and values of the past and present.”<sup>117</sup> While the Supreme Court continues to use the “actual (subjective) expectation of privacy” formulation, the Court has cautioned that in some situations it “provide[s] an inadequate index of Fourth Amendment protection.”<sup>118</sup> Arguably, therefore, greater emphasis should be placed on the *Katz* test’s second prong, which requires an individual’s expectation of privacy be one that society is prepared to recognize as reasonable.<sup>119</sup> The following cases explore the Court’s applications of the *Katz* test to law enforcement’s use of various electronic surveillance techniques.

### 3. Supreme Court Case Law Applying the *Katz* Test

#### a. United States v. Knotts

In *United States v. Knotts*,<sup>120</sup> narcotics officers were investigating defendants Darryl Petschen and Tristan Armstrong for the manufacturing of illegal drugs.<sup>121</sup> The officers discovered that Armstrong had been purchasing large quantities of chloroform, a solvent used to manufacture drugs, and delivering the chloroform to Petschen.<sup>122</sup> With the

---

117. *United States v. White*, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting).

118. *See Smith v. Maryland*, 442 U.S. 735, 740 n.5 (1979) (noting that the individual’s expectation of privacy must also be justifiable when viewed objectively).

119. *See Amsterdam*, *supra* note 66, at 384

An actual, subjective expectation of privacy . . . can neither add to, nor can its absence detract from, an individual’s claim to [F]ourth [A]mendment protection. If it could, the government could diminish each person’s subjective expectation of privacy merely by announcing half-hourly on television that . . . we were all forthwith being placed under comprehensive electronic surveillance.

120. 460 U.S. 276 (1983).

121. *See id.* at 278 (describing the process by which the 3M Company, a chemical manufacturing company, notified local law enforcement that one of its former employees had been stealing chemicals used to manufacture illegal drugs).

122. *See id.* (“Visual surveillance of Armstrong revealed that after leaving the employ of 3M Company, he had been purchasing similar chemicals from the Hawkins Chemical Company in Minneapolis.”).

chemical manufacturing company’s permission, the officers installed a beeper inside a container of chloroform, which the company later sold to Armstrong.<sup>123</sup> Using the beeper, the officers tracked the container to Leroy Knotts’s cabin in rural Wisconsin, where they discovered a clandestine drug operation.<sup>124</sup> Knotts and Petschen moved to suppress the evidence obtained as a result of the officers’ warrantless installation and monitoring of the beeper.<sup>125</sup> Their motion was denied by the United States District Court for the District of Minnesota.<sup>126</sup> A divided panel of the Court of Appeals for the Eighth Circuit reversed, holding that the evidence obtained from the search of Knotts’s cabin was admissible against Petschen, but not against Knotts.<sup>127</sup> Knotts appealed, and the Supreme Court granted certiorari.<sup>128</sup>

The issue presented to the Supreme Court was whether the officers’ “use of a beeper violated [Knotts’s] rights secured by the Fourth Amendment to the United States Constitution.”<sup>129</sup> The Court ultimately held that “[a] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.”<sup>130</sup> In so holding, the Court emphasized that by driving along public thoroughfares, Petschen “voluntarily

---

123. *See id.* (describing the agreement under which the Hawkins Chemical Company agreed to sell Armstrong a gallon of chloroform with a beeper inside it).

124. After crossing into Wisconsin, Petschen began making evasive maneuvers and the pursuing agents were forced to end their visual surveillance. The officers lost the beeper’s signal for almost an hour. The officers were only able to regain the signal with help from a monitoring device located in a helicopter. *Id.* at 278.

125. *Id.*

126. *See id.* (denying the motion to suppress and convicting Knotts for conspiring to manufacture controlled substances).

127. *See United States v. Knotts*, 662 F.2d 515, 518 (8th Cir. 1981) (explaining that Knotts, as the resident and owner of the property, had a reasonable, legitimate expectation of privacy in the cans of chloroform, but that Petschen’s expectation of privacy was not one society would be prepared to recognize as reasonable).

128. *United States v. Knotts*, 457 U.S. 1131 (1982).

129. *United States v. Knotts*, 460 U.S. 276, 278 (1983).

130. *Id.* at 281.

conveyed to anyone who wanted to look the fact that he was travelling over particular roads in a particular direction . . . and the fact of his final destination when he exited from public roads onto private property.”<sup>131</sup> The Court further explained that because the officers could have visually surveilled Petschen driving along public roads and onto Knotts’s property, “scientific enhancement of this sort raise[d] no constitutional issues which visual surveillance would not also raise.”<sup>132</sup>

The Court’s *Knotts* decision stands for three propositions, all of which are potentially relevant to an analysis of the Fourth Amendment issues raised by law enforcement’s use of cell-site simulators. First, the Fourth Amendment does not prohibit law enforcement officers from augmenting and enhancing their senses by using technology.<sup>133</sup> Second, a landowner does not have a reasonable expectation of privacy in the visual observations of an automobile arriving on his private premises after leaving a public highway.<sup>134</sup> Third, a homeowner does not have a reasonable expectation of privacy in the movements of objects outside his home in the “open fields.”<sup>135</sup>

---

131. *Id.* at 281–82.

132. *Id.* at 285.

133. *See id.* at 282 (“Nothing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case.”); *see also* *United States v. Lee*, 274 U.S. 559, 563 (1927) (holding that the use of a “searchlight” is “comparable to the use of a marine glass or a field glass” and “is not prohibited by the Constitution”).

134. *See id.* (“[N]o such expectation of privacy extended to the visual observation of Petschen’s automobile arriving on his premises after leaving a public highway . . .”).

135. *See id.* (“[N]o such expectation of privacy extended to the . . . movements of objects such as the drum of chloroform outside the cabin in the ‘open fields.’”); *see also* *Hester v. United States*, 265 U.S. 57, 59 (1924) (“[T]he special protection accorded by the Fourth Amendment to the people in their ‘persons, houses, papers and effects,’ is not extended to the open fields.”).

*b. United States v. Karo*

Building off of questions left unresolved by its decision in *Knotts*,<sup>136</sup> in *United States v. Karo*, the Supreme Court addressed whether the “monitoring of a beeper in a private residence, a location not open to visual surveillance, violates the Fourth Amendment rights of those who have a justifiable interest in the privacy of the residence.”<sup>137</sup> After receiving a tip that James Karo had ordered fifty gallons of ether, a compound often used in the manufacture of illegal drugs, DEA agents placed a beeper in one of the cans eventually sold to Karo.<sup>138</sup> Using the beeper, DEA agents were able to track the can of ether as it was moved from Karo’s own residence to other private residences.<sup>139</sup>

The Court applied the *Katz* test to the DEA agents’ monitoring of the beeper: “[P]rivate residences are places in which the individual normally expects privacy free of governmental intrusion not authorized by a warrant, and that expectation is plainly one that society is prepared to recognize as justifiable.”<sup>140</sup> The Court went on to hold that the agents’ monitoring of the beeper was a Fourth Amendment search.<sup>141</sup> In so holding, the Court relied on the “general rule that a search of a house should be conducted pursuant to a

---

136. In *Knotts*, the record did not show that law enforcement had been monitoring the beeper while the can of chloroform was inside Knotts’s cabin. Thus, the Court “had no occasion to consider whether a constitutional violation would have occurred had the fact been otherwise.” *United States v. Karo*, 468 U.S. 705, 714 (1984).

137. *Id.*

138. *See id.* at 708 (explaining that ether is used to extract cocaine from clothing).

139. *See id.* (describing the can’s movements from Karo’s residence to Horton’s residence, from Horton’s residence to his father’s residence, and finally, from Horton’s father’s residence to a commercial storage facility).

140. *Id.* at 714.

141. *See id.*

This case thus presents the question whether the monitoring of a beeper in a private residence, a location not open to visual surveillance, violates the Fourth Amendment rights of those who have a justifiable interest in the privacy of the residence. Contrary to the submission of the United States, we think that it does.

warrant.”<sup>142</sup> The Court distinguished *Karo* from *Knotts* on the grounds that no constitutionally protected area was implicated by the law enforcement officers’ surveillance in *Knotts*, whereas the beeper surveillance in *Karo* allowed law enforcement to monitor the can of ether inside *Karo*’s residence.<sup>143</sup> Unlike the surveillance information obtained in *Knotts*, the beeper monitoring in *Karo* “reveal[ed] a critical fact about the interior of the premises that the Government [was] extremely interested in knowing and that it could not have otherwise obtained without a warrant.”<sup>144</sup>

Taken together, the Court’s decisions in *Knotts* and *Karo* indicate that law enforcement’s warrantless use of an electronic beeper to monitor an individual’s movements is not a search if the monitoring reveals information that was “voluntarily conveyed to anyone who wanted to look.”<sup>145</sup> If, however, law enforcement’s warrantless monitoring infringes on a constitutionally protected area, such as the home, then law enforcement have engaged in a Fourth Amendment search.<sup>146</sup>

### c. *Kyllo v. United States*

In *Kyllo v. United States*, DEA agents directed a thermal imager<sup>147</sup> at the side of Danny *Kyllo*’s residence in order to

---

142. *Id.* at 718.

143. *See id.* at 715 (emphasizing that by monitoring the beeper, the agents knew that the can was inside *Karo*’s residence, something they could not have verified visually).

144. *Id.*

145. *See id.* (“The information obtained in *Knotts* was ‘voluntarily conveyed to anyone who wanted to look’; here, as we have said, the monitoring indicated that the beeper was inside the house, a fact that could not have been visually verified.” (quoting *United States v. Knotts*, 460 U.S. 276, 281 (1983))).

146. *See Freiwald & Smith, supra* note 54, at 207 (“*Knotts* and *Karo* brought needed clarity . . . [a] dividing line was drawn between public and private space—tracking a vehicle on a public highway was not a search, but monitoring a device within the home or other constitutionally protected space was subject to Fourth Amendment constraints.”).

147. *See Kyllo v. United States*, 533 U.S. 27, 29–30 (2001) (describing a thermal imager as a device that converts radiation into images based on

ascertain whether Kyllo was growing marijuana in his home.<sup>148</sup> Scans from the thermal imager showed that the roof over Kyllo’s garage was “relatively hot compared to the rest of the home and substantially warmer than neighboring homes in the triplex.”<sup>149</sup> The agents concluded that Kyllo was using halide lights to grow marijuana.<sup>150</sup> Based in part on the thermal imager’s scans, the agents were able to obtain a warrant to search Kyllo’s home.<sup>151</sup> The agents’ search revealed an indoor growing operation of more than one hundred marijuana plants.<sup>152</sup> Kyllo moved to suppress all evidence obtained as a result of the agents’ search.<sup>153</sup>

The issue for the Supreme Court’s consideration was whether the DEA agents’ use of a thermal imager directed at a private home from a public street constituted a Fourth Amendment search.<sup>154</sup> The Court held that the information obtained via the thermal imager was the product of a search.<sup>155</sup> Specifically, the agents engaged in a search when they obtained “by sense-enhancing technology . . . information regarding the interior of the home that could not otherwise have been obtained without physical intrusion into a constitutionally protected area.”<sup>156</sup>

---

relative degrees of warmth: “black is cool, white is hot, shades of gray connote relative differences”).

148. *See id.* at 29 (“Agent William Elliott of the United States Department of the Interior came to suspect that marijuana was being grown in the home belonging to . . . Danny Kyllo.”).

149. *Id.* at 30.

150. *Id.*

151. *See id.* (noting that the magistrate judge also relied on tips from informants and Kyllo’s utility bills in granting the requested search warrant).

152. *Id.*

153. *Id.*

154. *See id.* at 33 (emphasizing that the case involved more than “naked-eye” surveillance of a home).

155. *See id.* at 40 (“Where, as 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.”).

156. *Id.* at 34.

In so holding, the *Kyllo* Court expressed its concern regarding the effects advances in technology have had and would continue to have on individuals' expectations of privacy.<sup>157</sup> One of the questions the Court sought to answer was, given the circularity of the *Katz* test,<sup>158</sup> "what limits there are upon [the] power of technology to shrink the realm of guaranteed privacy."<sup>159</sup> According to the Court, the answer, at least with regard to the interior of the home, lay in a "ready criterion": protection of the interior of the home has "roots deep within the common law" and has been "acknowledged to be reasonable."<sup>160</sup> The Court concluded that because the thermal imager revealed information regarding the interior of *Kyllo's* home that "could not otherwise have been obtained without physical intrusion,"<sup>161</sup> the use of the thermal imager constituted a search.<sup>162</sup>

*d. United States v. Jones*

In *United States v. Jones*, FBI agents were investigating Antoine Jones's suspected involvement in a large-scale drug trafficking organization.<sup>163</sup> In the thirty years between the Supreme Court's decisions in *Knotts* and *Karo* and its decision in *Jones*, surveillance technology has made significant

---

157. See *id.* at 33–34 ("It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology.").

158. See, e.g., Richard A. Posner, *The Uncertain Protection of Privacy by the Supreme Court*, 1979 SUP. CT. REV. 173, 188 (1979) ("And it is circular to say that there is no invasion of privacy unless the individual whose privacy is invaded had a reasonable expectation of privacy; whether he will or will not have such an expectation will depend on what the legal rule is.").

159. *Kyllo v. United States*, 533 U.S. 27, 34 (2001).

160. *Id.*

161. *Id.*

162. See *id.* (acknowledging critiques of the *Katz* test but noting that withdrawing protection of the expectation of privacy an individual has in his home in this case would effectively "permit police technology to erode the privacy guaranteed by the Fourth Amendment").

163. See *United States v. Jones*, 565 U.S. 400, 402 (2012) ("In 2004 respondent Antoine Jones, owner and operator of a nightclub in the District of Columbia, came under suspicion of trafficking in narcotics and was made the target of an investigation . . .").

advances. Where the law enforcement officers in *Knotts* and *Karo* relied on electronic beepers to monitor their suspects, FBI agents were able to track Jones for twenty-eight straight days after they affixed a GPS tracking device to his vehicle.<sup>164</sup> Although the *Jones* Court was faced with an issue raised by more sophisticated surveillance technology, it relied on the traditional, physical trespass test in holding that the FBI agents’ placement and subsequent monitoring of the GPS tracking device on Jones’s vehicle constituted a search.<sup>165</sup>

Justice Sotomayor, writing in concurrence, emphasized that although she agreed with the majority’s trespass analysis,<sup>166</sup> surveillance cases like the one at issue should be analyzed under the *Katz* test because “physical intrusion is now unnecessary to many forms of surveillance.”<sup>167</sup> In support of her assertion, Justice Sotomayor called attention to the issues raised by GPS monitoring, including the “precise, comprehensive record” it generates, the detail regarding an individual’s “familial, political, professional, religious, and sexual associations” it reveals, and the ease with which it can be carried out.<sup>168</sup> Justice Sotomayor urged that the GPS device’s capabilities be taken into account when “considering a reasonable societal expectation of privacy in the sum of one’s public movements.”<sup>169</sup> According to Justice Sotomayor, in examining whether GPS monitoring constitutes a search, courts should consider “whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, [and] sexual habits.”<sup>170</sup>

---

164. *Id.* at 403.

165. *See 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.’”).

166. *See id.* (Sotomayor, J., concurring) (“By contrast, the trespassory test applied in the majority’s opinion reflects an irreducible constitutional minimum: When the Government physically invades personal property to gather information, a search occurs.”).

167. *Id.*

168. *Id.* at 415–16.

169. *Id.* at 416.

170. *Id.*



Like Justice Sotomayor, Justice Alito argued in favor of a *Katz* analysis to determine whether the FBI agents had engaged in a search.<sup>171</sup> Justice Alito placed particular emphasis on the “lengthy monitoring that occurred in this case,”<sup>172</sup> noting that relatively short-term monitoring of a person’s movements in public does not violate the Fourth Amendment.<sup>173</sup> Justice Alito was most concerned with the ease and detail with which the FBI agents were able to track Jones: “[F]or four weeks, law enforcement agents tracked every movement that respondent made in the vehicle he was driving.”<sup>174</sup> Although he was unwilling to “identify with precision the point at which the tracking of this vehicle became a search,” Justice Alito concluded that the “line was surely crossed before the 4-week mark.”<sup>175</sup> Justice Alito proposed that, in future cases, courts ask “whether the use of GPS tracking in a particular case involve[s] a degree of intrusion that a reasonable person would not have anticipated.”<sup>176</sup> Justice Ginsburg, Justice Breyer, and Justice Kagan joined in Justice Alito’s concurrence. Thus, according to five Justices, because GPS monitoring tracks “every movement” an individual makes, “longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.”<sup>177</sup>

*e. Carpenter v. United States*

In *Carpenter v. United States*, FBI agents obtained 127 days’ worth of defendant Timothy Carpenter’s CSLI during

---

171. See *id.* at 419 (Alito, J., concurring) (arguing the Court should have “analyze[d] the question presented in this case by asking whether respondent’s reasonable expectations of privacy were violated”).

172. *Id.* at 431.

173. *Id.* at 430.

174. *Id.*

175. *Id.*

176. *Id.*

177. *Id.* (Alito, J., concurring); *id.* at 415 (Sotomayor, J., concurring); see also *Carpenter v. United States*, 138 S. Ct. 2206, 2215 (2018) (citing to the two concurrences in *Jones* to support the proposition that longer term GPS monitoring “impinges on expectations of privacy”—regardless of whether those movements were disclosed to the public at large).

their investigation into a string of robberies.<sup>178</sup> After the prosecution identified Carpenter as one of the accomplices who had participated in the heists,<sup>179</sup> a magistrate judge ordered MetroPCS and Sprint to “disclose ‘cell/site sector [information] for [Carpenter’s] telephone[] at call origination and at call termination for incoming and outgoing calls’ during the four-month period when the string of robberies occurred.”<sup>180</sup> Using Carpenter’s CSLI, the prosecution was able to retroactively place Carpenter’s cell phone near the location of the robberies at the date and time each robbery took place.<sup>181</sup> At trial, Carpenter moved to suppress the CSLI.<sup>182</sup> The District Court for the Eastern District of Michigan denied Carpenter’s motion,<sup>183</sup> and the Sixth Circuit affirmed.<sup>184</sup> Carpenter then appealed to the Supreme Court.<sup>185</sup>

The Supreme Court reversed the Sixth Circuit, holding that the location information obtained from Carpenter’s wireless carriers was the product of a search, and that law enforcement must generally obtain a warrant supported by probable cause before obtaining CSLI.<sup>186</sup> The Court applied the

---

178. See *Carpenter v. United States*, 138 S. Ct. 2206, 2212 (2018) (describing as “ironic” the string of robberies of Radio Shack and T-Mobile stores in Michigan and Ohio).

179. *Id.*

180. *Id.* (citation omitted).

181. See *id.* at 2213 (explaining the FBI agent’s process of using Carpenter’s CSLI to generate maps placing Carpenter’s cell phone near four of the charged robberies).

182. See *id.* at 2212 (arguing that the government’s seizure of Carpenter’s CSLI records violated his Fourth Amendment rights because they had been obtained without a warrant supported by probable cause).

183. See *United States v. Carpenter*, No. 12–20218, 2013 WL 6385838, at \*6 (E.D. Mich., Dec. 6, 2013) (denying Carpenter’s motion to suppress his CSLI and his motion seeking to preclude the expert testimony of the FBI special agent who generated the maps placing Carpenter’s cell phone near the sites of the robberies).

184. *United States v. Carpenter*, 819 F.3d 880 (6th Cir. 2016).

185. See *Carpenter v. United States*, 137 S. Ct. 2211 (2017) (granting certiorari).

186. See *Carpenter*, 138 S. Ct. at 2221 (“Having found that the acquisition of Carpenter’s CSLI was a search, we also conclude that the Government must generally obtain a warrant supported by probable cause before acquiring such records.”).

*Katz* reasonable expectation of privacy test, noting that CSLI implicates an individual's expectation of privacy in both his "physical location and movements" and "in information voluntarily turned over to third parties."<sup>187</sup> The Court held that Carpenter "maintain[ed] a legitimate expectation of privacy in the record of his physical movements as captured through CSLI,"<sup>188</sup> and that law enforcement's access of seven days' worth of Carpenter's CSLI constituted a Fourth Amendment search.<sup>189</sup>

In so holding, the Court compared law enforcement's use of CSLI to GPS monitoring, noting that the "detailed, encyclopedic, and effortlessly compiled" data used to track a person via their CSLI was qualitatively similar to the GPS monitoring in *Jones*.<sup>190</sup> Like GPS monitoring, access to CSLI is "remarkably easy, cheap, and efficient compared to traditional investigative tools."<sup>191</sup> Arguably, however, law enforcement's use of CSLI raises even greater privacy concerns than the GPS monitoring in *Jones* because cell phones are almost "feature[s] of human anatomy" that track the movements of their users

---

187. See *id.* at 2214–15 ("[R]equests for cell-site records lie at the intersection of two lines of cases, both of which inform our understanding of the privacy interests at stake."); see also *Smith v. Maryland*, 442 U.S. 735, 743 (1979) (holding that an individual does not have a reasonable expectation of privacy in the records of his dialed telephone numbers held by the individual's telephone company); *United States v. Miller*, 425 U.S. 435, 444–45 (1976) (holding that an individual does not have a reasonable expectation of privacy in financial records voluntarily disclosed to a bank). Compare *United States v. Jones*, 565 U.S. 400, 430 (2012) (Alito, J., concurring) (concluding that privacy concerns would be raised by GPS tracking), with *United States v. Knotts*, 460 U.S. 276, 281 (1983) (holding that "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another").

188. See *Carpenter*, 138 S. Ct. at 2217 (explaining that the seven days' worth of CSLI from Sprint was the "pertinent period").

189. See *id.* at 2217 n.3 (responding to the alternative argument that "the acquisition of CSLI becomes a search only if it extends beyond a limited period").

190. See *id.* at 2216 (analogizing law enforcement's use of CSLI in this case to the GPS tracking of a vehicle; in both instances, the location information is "detailed, encyclopedic, and effortlessly compiled").

191. *Id.* at 2218.

“nearly exactly.”<sup>192</sup> Additionally, the retrospective nature of CSLI grants law enforcement access to historical location information, “a category of information [that is] otherwise unknowable.”<sup>193</sup>

*4. Case Law Applying the Katz Test to Law Enforcement’s Use of Cell-Site Simulators*

*a. Maryland v. Andrews*

In *Maryland v. Andrews*, the Court of Special Appeals of Maryland considered whether “the use of a cellular tracking device to locate Andrews’s phone violated the Fourth Amendment.”<sup>194</sup> Baltimore police had used a cell-site simulator to locate Andrews at an acquaintance’s apartment.<sup>195</sup> The court concluded that “individuals have a reasonable expectation that their cell phones will not be used as real-time tracking devices by law enforcement, and—recognizing that the Fourth Amendment protects people and not simply areas—that people have an objectively reasonable expectation of privacy in real-time cell phone location information.”<sup>196</sup> According to the *Andrews* court, therefore, “the use of a cell-site simulator . . . by the government, requires a search warrant based on probable cause and describing with particularity the object and manner of the search, unless an established exception to the warrant requirement applies.”<sup>197</sup>

In holding that Andrews had a reasonable expectation of privacy in the location information obtained by the cell-site

---

192. See *Riley v. California*, 573 U.S. 373, 385 (2014) (“[T]he proverbial visitor from Mars might conclude [cell phones] were an important feature of human anatomy.”).

193. *Carpenter v. United States*, 138 S. Ct. 2206, 2218 (2018).

194. *Maryland v. Andrews*, 134 A.3d 324, 326 (Ct. Spec. App. Md. 2016).

195. The Government also argued that Andrews lacked standing to challenge the search because Andrews did not have a reasonable expectation of privacy in an acquaintance’s residence. The *Andrews* court refused to rule on the standing argument because it had “already determined that Andrews had a reasonable expectation of privacy in his aggregate and real-time location information (CSLI) contained in his cell phone.” *Id.* at 352–53.

196. *Id.* at 327.

197. *Id.* at 395.

simulator, the *Andrews* court rejected two propositions.<sup>198</sup> First, the court rejected the idea that cell phone users voluntarily convey their location information simply by choosing to use their cell phones and to carry the devices on their person.<sup>199</sup> Second, the court dismissed the proposition that cell phone users should expect that their information is being sent directly to the police department.<sup>200</sup>

*b. United States v. Lambis*

In *United States v. Lambis*, the United States District Court for the Southern District of New York also held that law enforcement must obtain a search warrant supported by probable cause before using a cell-site simulator.<sup>201</sup> DEA agents obtained Lambis's cell phone number as part of their investigation into an international drug trafficking organization.<sup>202</sup> The agents initially used CSLI to determine the approximate location of Lambis's cell phone, but the CSLI was not precise enough to identify Lambis's apartment building.<sup>203</sup> Using a cell-site simulator, a trained DEA technician located Lambis's apartment building and specific apartment by isolating the signal emanating from Lambis's

---

198. *Id.* at 392–93.

199. *See id.* at 392 (agreeing with the Fourth Circuit's decision in *United States v. Graham* that courts "cannot accept the proposition that cell phone users volunteer to convey their location information simply by choosing to activate and use their cell phones and to carry the devices on their person" (quoting *United States v. Graham*, 796 F.3d 332, 355 (4th Cir. 2015), *cert. denied*, 138 S. Ct. 2700 (2018))).

200. *See id.* at 392–93 (accepting the circuit court's finding that "no one expects that their phone information is being sent directly to the police department on their apparatus").

201. *See United States v. Lambis*, 197 F. Supp. 3d 609, 610 (S.D.N.Y. 2016) (explaining that, in light of *Kyllo*, DEA agents' use of a cell-site simulator to locate Lambis's apartment was an "unreasonable search because the 'pings' from Lambis's cell phone to the nearest cell site were not readily available 'to anyone who wanted to look' without the use of a cell-site simulator").

202. *Id.* at 609.

203. *See id.* (describing the CSLI as not precise enough to identify Lambis's specific apartment building, much less the specific unit in the apartment complexes in the area).

cell phone.<sup>204</sup> Later that same day, Lambis’s father gave the agents consent to enter the apartment,<sup>205</sup> where they recovered narcotics and other drug paraphernalia from Lambis’s bedroom.<sup>206</sup> Lambis filed a motion to suppress the evidence of drugs and drug paraphernalia.<sup>207</sup>

The court held that the DEA agents’ warrantless use of a cell-site simulator constituted an unreasonable search in violation of the Fourth Amendment.<sup>208</sup> Relying heavily on the Supreme Court’s decision in *Kyllo*,<sup>209</sup> the *Lambis* court reasoned that the agents’ use of the cell-site simulator was a search because the “‘pings’ from Lambis’s cell phone . . . were not readily available ‘to anyone who wanted to look.’”<sup>210</sup>

c. *Jones v. United States*

In *Jones v. United States*, officers from the D.C. Metropolitan Police Department used a cell-site simulator to track a suspect wanted for two sexual assaults.<sup>211</sup> The officers

---

204. *See id.* (“Activating the cell-site simulator, the DEA technician first identified the apartment building with the strongest ping. Then, the technician entered that apartment building and walked the halls until he located the specific apartment where the signal was strongest.”).

205. *See id.* (noting that Lambis himself also gave his consent when DEA agents asked to search his bedroom).

206. *See id.* (detailing the DEA agents’ seizure of narcotics, three digital scales, empty zip lock bags, and other drug paraphernalia from Lambis’s bedroom).

207. *Id.*

208. *See id.* at 611 (discussing the special significance afforded to the home under the Fourth Amendment); *Kyllo v. United States*, 533 U.S. 27, 31 (2001) (“‘At the very core’ of the Fourth Amendment ‘stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.’” (citation omitted)).

209. *See Kyllo*, 533 U.S. at 40 (holding that when “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”).

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

211. *See Jones v. United States*, 168 A.3d 703, 707 (D.C. Ct. App. 2017) (recounting that the officers’ review of the two victims’ phone records revealed they both had received phone calls from Jones).

believed their suspect, Jones, had stolen one of the victim's cell phones.<sup>212</sup> To further their investigation, the officers sought and obtained real-time CSLI from both Jones's and the victim's telecommunications providers.<sup>213</sup> This information placed the two cell phones in the general vicinity of the Minnesota Avenue Metro Station.<sup>214</sup> In order to better pinpoint the locations of the two cell phones, the officers drove a truck equipped with a cell-site simulator around the station.<sup>215</sup> Using the cell-site simulator, the officers tracked Jones's cell phone's signal to a parked vehicle.<sup>216</sup> "Inside the [vehicle] were Mr. Jones and Mr. Jones's girlfriend, Nora Williams."<sup>217</sup>

The D.C. Circuit Court of Appeals held that the officers' use of the cell-site simulator to locate Jones's phone "invaded [his] reasonable expectation of privacy and was thus a search."<sup>218</sup> The court began its analysis with an "obvious fact": "[M]ost people have a cellphone and carry it with them practically everywhere they go."<sup>219</sup> According to the court, because cell phone usage is so pervasive, cell-site simulators have "substantial potential to expose the [cell phone] owner's intimate personal information."<sup>220</sup> Cell phone tracking can, for example, invade the cell phone owner's "right to privacy in one's home"<sup>221</sup> and can reveal "sensitive information about the

---

212. *Id.*

213. *See id.* at 708 (explaining that the information came in the form of geographic coordinates that lacked a high degree of certainty).

214. *See id.* ("Despite the lack of precision in the location information, Sergeant Perkins and his team were able to 'tell that . . . one of the [complainants'] phones and the [suspect's] phone were traveling in the same general direction . . . as if they were together.'" (citation omitted)).

215. *Id.*

216. *Id.* at 709.

217. *Id.*

218. *Id.* at 713.

219. *Id.* at 711 (citing *Riley v. California*, 573 U.S. 373, 395 (2014)) ("Finally, there is an element of pervasiveness that characterizes cell phones . . . [n]ow it is the person who is not carrying a cell phone, with all that it contains, who is the exception.").

220. *Id.*

221. *Id.*

[owner’s] ‘familial, political, professional, religious, and sexual associations.’”<sup>222</sup>

The court walked through two additional considerations. First, the court sought to distinguish cell-site simulators from other electronic surveillance tools. Unlike the beepers used in *Knotts* and *Karo*, “a cell-site simulator is a locating, not merely a tracking device.”<sup>223</sup> Thus, “[w]ith a cell-site simulator . . . police no longer need to track a person visually from some starting location or physically install a tracking device on an object that is, or will come into, his or her possession.”<sup>224</sup> Second, the court emphasized that because cell phones are “dumb devices,” cell phone users are not able to insulate themselves from cell-site simulators.<sup>225</sup> The only countermeasure a cell phone user “can undertake is to turn off his or her cellphone or its radios (put it in ‘airplane mode’), thus forgoing its use as a communication device.”<sup>226</sup> The court concluded that, taken together, the information law enforcement can obtain by using a cell-site simulator and the means by which cell-site simulator surveillance is carried out mandates “that under ordinary circumstances, the use of a cell-site simulator to locate a person through his or her cellphone invades the person’s actual, legitimate, and

---

222. *Id.* at 712. The court is relying on Justice Sotomayor’s concurrence in *United States v. Jones*. *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring). In *Jones*, the government tracked Antoine Jones’s movements for four weeks. *Id.* at 403. Here, the officers used the cell-site simulator to track Prince Jones’s movements for only a few hours. *See Jones v. United States*, 168 A.3d 703, 709 (D.C. Ct. App. 2017) (describing the arrest of Prince Jones as taking place at 11:30 AM on the same day that the officers deployed the cell-site simulator).

223. *Id.* at 713.

224. *Id.* at 712.

225. *See id.* at 713

[T]he cell-site simulator exploits a security vulnerability in the phone—the fact that cellphones are, in the words of the defense expert, “dumb devices,” unable to differentiate between a legitimate cellular tower and a cell-site simulator masquerading as one—and actively induces the phone to divulge its identifying information. Once the phone is identified, it can be located.

(citation omitted).

226. *Id.*



reasonable expectation of privacy in his or her location information and is a search.”<sup>227</sup>

### *III. Four Factors Courts Should Consider When Analyzing Law Enforcement’s Use of a Cell-Site Simulator*

Taken together, *Andrews*, *Lambis*, and *Jones (D.C.)* indicate that when law enforcement officers use a cell-site simulator, they conduct a search within the meaning of the Fourth Amendment. To the extent these cases suggest that law enforcement’s use of cell-site simulators always amounts to a Fourth Amendment search, these holdings are overly-broad and rest on “too-generic description[s] of the facts.”<sup>228</sup> This Note proposes that courts should consider the following factors in determining, on a case-by-case basis,<sup>229</sup> whether law enforcement’s use of a cell-site simulator constituted a search: (1) whether the surveillance infringed on a constitutionally protected area, (2) the duration of the surveillance, (3) whether the surveillance was active or passive, and (4) the nature of the information obtained by the surveillance.<sup>230</sup>

---

227. *Id.* at 714–15.

228. *See id.* at 728 (Thompson, J., dissenting) (arguing that, despite the commendable concern about threats to privacy that flow from advances in law enforcement technology, the court’s conclusion was based on a “too-generic description of the facts surrounding use of the cell-site simulator”).

229. *See Warshak v. United States*, 532 F.3d 521, 528 (6th Cir. 2008) (“The Fourth Amendment is designed to account for an unpredictable and limitless range of factual circumstances, and accordingly it *generally* should be applied after those circumstances unfold, not before.” (emphasis added)); Brief of Professor Orin S. Kerr as Amicus Curiae Supporting Appellant, *In re United States for Historical Cell Site Data*, 724 F.3d 600 (5th Cir. 2013) (No. 11-20884) (arguing that ex post review of law enforcement’s actions is “essential because Fourth Amendment law is extremely fact-specific” and courts “cannot apply the Fourth Amendment when no facts yet exist”).

230. The *Kyllo* Court emphasized that a thermal imager is a sophisticated device that is “not in general public use.” *Kyllo v. United States*, 533 U.S. 27, 40 (2001). Like thermal imagers, cell-site simulators are highly sophisticated devices that are not generally available to the public. *See Brown & Leese, supra* note 35, at 12 (describing both the non-disclosure agreements imposed by Harris Corporation, the primary manufacturer of cell-site simulators, and the hefty purchase price—one cell-site simulator

*A. Whether the Surveillance Infringed on a Constitutionally Protected Area*

The first factor courts should consider when analyzing a case involving a cell-site simulator is whether law enforcement officers used the cell-site simulator to monitor an individual in a constitutionally protected area, such as the home.<sup>231</sup> If, by using the cell-site simulator, law enforcement officers obtain information regarding the interior of an individual’s home, then a Fourth Amendment search has taken place.<sup>232</sup> In such cases, courts need not consider the remaining factors and can instead proceed to analyze the reasonableness of the search.<sup>233</sup> Thus, to the extent that the *Lambis* court relied on an individual’s right to “retreat into his own home and there be free from unreasonable governmental intrusion,”<sup>234</sup> it was correct in concluding that law enforcement’s warrantless use of

---

costs around \$100,000). Thus, the sophisticated nature of cell-site simulators is a constant and does not need to be considered as an independent factor.

231. See *Kyllo*, 533 U.S. at 37 (“The Fourth Amendment’s protection of the home has never been tied to measurement of the quality or quantity of information obtained. In *Silverman*, for example, we made clear that any physical invasion of the structure of the home, ‘by even a fraction of an inch,’ was too much . . .” (quoting *Silverman v. United States*, 365 U.S. 505, 512 (1961))).

232. See *id.* (“In the home, our cases show, *all* details are intimate details, because the entire area is held safe from prying government eyes.”); *United States v. Karo*, 468 U.S. 705, 716 (1984) (holding that by using a beeper to monitor a private residence, law enforcement officers violated the Fourth Amendment rights of those individuals with privacy interests in the residence).

233. See *id.* at 31 (relying on the foundational notion that, at its very core, the Fourth Amendment protects “the right of man to retreat into his own home and there be free from unreasonable governmental intrusion” (citing *Silverman v. United States*, 365 U.S. 505, 511 (1961))); *Brown & Leese*, *supra* note 35, at 14 (arguing that if the “searches in *Karo* and *Kyllo* were in violation of the Fourth Amendment, so too would be the use of a cell-site simulator to track a cell phone inside a person’s home”); see also *New Jersey v. T.L.O.*, 469 U.S. 325, 340 (1985) (emphasizing that reasonableness is the “fundamental command” of the Fourth Amendment).

234. *Silverman v. United States*, 365 U.S. 505, 511 (1961).

a cell-site simulator violated Lambis's reasonable expectation of privacy.<sup>235</sup>

If, however, the cell-site simulator does not reveal information regarding the interior of an individual's home,<sup>236</sup> then additional analysis is required.<sup>237</sup> Recall that under *Knotts*, for example, surveilling an individual in public is not a search within the meaning of the Fourth Amendment.<sup>238</sup>

---

235. See *United States v. Lambis*, 197 F. Supp. 3d 606, 610 (S.D.N.Y. 2016) ("The DEA's use of the cell-site simulator revealed details of the home that would previously have been unknowable without physical intrusion, namely, that the target cell phone was located within Lambis's apartment." (citation omitted)). The *Lambis* Court should have limited its holding to these facts, but instead held that "[a]bsent a search warrant, the Government may not turn a citizen's cell phone into a tracking device." *Id.* at 611.

236. *Andrews* presents an interesting question: did Andrews have the same expectations of privacy in an acquaintance's apartment as he would have had in his own home? Put differently, did Andrews have standing to bring a Fourth Amendment claim? The *Andrews* court declined to address the standing issue because it had "already determined that Andrews had a reasonable expectation of privacy in his . . . location information . . . contained in his cell phone." *Maryland v. Andrews*, 134 A.3d 324, 353 (Ct. Spec. App. Md. 2016). In future cell-site simulator questions, however, courts should be prepared to analyze whether the target is able to establish "that his own Fourth Amendment rights were violated by the challenged search." *Rakas v. Illinois*, 439 U.S. 128, 130 n.1 (1978).

237. See, e.g., *United States v. Griffin*, 729 F.2d 475, 483–84 (7th Cir. 1984) (holding that individuals have a reduced expectation of privacy in automobiles because automobiles are subject to pervasive and continuing governmental regulation); see also LAFAVE, *supra* note 64, § 11.3(b) (discussing reasonable expectations of privacy in residential premises). Compare *Minnesota v. Olson*, 495 U.S. 91, 96–97 (1990) (holding that one's "status as an overnight guest is alone enough to show . . . an expectation of privacy in the home that society is prepared to recognize as reasonable"), with *Minnesota v. Carter*, 525 U.S. 83, 90 (1998) (holding that two visitors who came to an apartment for the sole purpose of packaging the cocaine, had never been to the apartment before, and were only in the apartment for 2.5 hours lacked standing to challenge an officer's search of the apartment).

238. See *United States v. Knotts*, 460 U.S. 276, 285 (1983) (explaining that because the officers could have visually surveilled the defendant while he was driving in public, the "enhancement of their senses" provided by the beeper "raise[d] no constitutional issues which visual surveillance would not also raise").

*B. The Duration of the Surveillance*

The duration of law enforcement’s surveillance was a significant factor for the Supreme Court in both *United States v. Jones* and *Carpenter v. United States*. Accordingly, the second factor courts should consider in analyzing a cell-site simulator case is the duration of the cell-site simulator surveillance. In *Jones*, law enforcement surveilled Jones’s movements for four weeks by installing a GPS tracking device on his vehicle.<sup>239</sup> Writing in concurrence, Justice Alito concluded that the “lengthy monitoring in this case constituted a search under the Fourth Amendment.”<sup>240</sup> In *Carpenter*, FBI agents obtained 127 days’ worth of Carpenter’s CSLI.<sup>241</sup> Although the *Carpenter* Court refrained from issuing a bright line rule regarding precisely how many days’ worth of CSLI constitute a Fourth Amendment search,<sup>242</sup> it concluded that “accessing seven days of CSLI constitutes a Fourth Amendment search.”<sup>243</sup>

The cell-site simulator surveillance at issue in *Andrews*, *Lambis*, and *Jones (D.C.)* was nowhere near as lengthy as the surveillance in *Jones* or *Carpenter*. Generally, law enforcement officers use cell-site simulators as a last resort in their surveillance arsenal, only after they have been tracking a target for some time or are already aware of a target’s general location. In *Andrews*, for example, officers obtained Andrews’s

---

239. See *United States v. Jones*, 565 U.S. 400, 403 (2001) (“Over the next 28 days, the Government used the device to track the vehicle’s movements.”).

240. *Id.* at 431.

241. See *Carpenter v. United States*, 138 S. Ct. 2206, 2212 (2018) (describing the magistrate judge’s order to MetroPCS, which produced 127 days’ worth of Carpenter’s cell phone records).

242. See *id.* at 2217 n.3 (declining to decide whether there is a “limited period for which the Government may obtain an individual’s historical CSLI free from Fourth Amendment scrutiny”); see also *Jones*, 565 U.S. at 430 (“We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark.”).

243. *Carpenter*, 138 S. Ct. at 2217 n.3.

CSLI for the period from April 5 to May 5, pen register<sup>244</sup> data for a period of sixty days, and precision GPS data from Andrews's cell phone before ever using the cell-site simulator.<sup>245</sup> After tracking Andrews's cell phone's location to "the area of 5000 Clifton Avenue," the officers deployed the cell-site simulator, which was able to pinpoint the cell phone's location as "inside the residence at 5032 Clifton Avenue."<sup>246</sup> The whole process took no more than a few hours. Cell-site simulators were used for similarly brief periods of time in *Lambis* and *Jones (D.C.)*.<sup>247</sup> Thus, under *Jones* and *Carpenter*, the generally brief duration of cell-site simulator surveillance should cut against a finding that law enforcement's use of a cell-site simulator constituted a Fourth Amendment search.

### *C. Active Versus Passive Surveillance*

Courts should also consider the distinction between active, labor-intensive surveillance and passive surveillance when analyzing whether law enforcement's use of a cell-site simulator constituted a search.<sup>248</sup> The Supreme Court has often emphasized the ease with which surveillance can be carried out when balancing the government's interest in surveillance against an individual's expectations of privacy.<sup>249</sup>

---

244. See *United States v. N.Y. Tel. Co.*, 434 U.S. 159, 161 n.1 (1977) ("A pen register is a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released. It does not overhear oral communications and does not indicate whether calls are actually completed.")

245. *Maryland v. Andrews*, 134 A.3d 324, 328 (Ct. Spec. App. Md. 2016).

246. *Id.* at 329.

247. See *Jones v. United States*, 168 A.3d 703, 708 (D.C. Ct. App. 2017) (describing the officers driving around the area of a specified metro station with a cell-site simulator in the back of their vehicle); *United States v. Lambis*, 197 F. Supp. 3d 606, 609 (S.D.N.Y. 2016) (describing the DEA technician walking the halls of Lambis's apartment building with a cell-site simulator).

248. The distinction between active and passive surveillance should not be confused with the distinction between active and passive cell-site simulators. See *supra* notes 44–49 and accompanying text (discussing the differences between active and passive cell-site simulators).

249. See *United States v. Jones*, 565 U.S. 400, 415–16 (2012) (Sotomayor, J., concurring) ("[B]ecause GPS monitoring is cheap in comparison to

Whereas prolonged surveillance was difficult, costly, and therefore rarely undertaken in the “pre-computer age,” technological advances have allowed law enforcement to surveil more targets while expending less time and fewer resources.<sup>250</sup>

As noted by Justice Alito in *Jones*, without a GPS device, surveilling Jones’s vehicle for four weeks would have “required a large team of agents, multiple vehicles, and perhaps aerial surveillance.”<sup>251</sup> Thus, “[o]nly an investigation of unusual importance could have justified such an expenditure of law enforcement.”<sup>252</sup> By placing a GPS tracking device on Jones’s vehicle, however, law enforcement officers were able to passively track the vehicle’s movements for twenty-eight days.<sup>253</sup> Passive surveillance was also an issue for the *Carpenter* Court, where Chief Justice Roberts likened GPS tracking to law enforcement’s use of CSLI: both are inexpensive and “remarkably easy.”<sup>254</sup> In *Carpenter*, FBI agents were able to access a comprehensive catalogue of Carpenter’s historical location information with “just the click of a button.”<sup>255</sup> Under both *Jones* and *Carpenter*, the Court indicated that when technology enables law enforcement to surveil a target passively, for extended periods of time, such technology is more likely to violate the reasonableness mandate of the Fourth Amendment.

---

conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices.”); *Illinois v. Lidster*, 540 U.S. 419, 427 (2004) (balancing the gravity of the public interest and the severity of the interference with individual liberty in determining the reasonableness of a checkpoint stop).

250. *Jones*, 565 U.S. at 429 (Alito, J., concurring).

251. *Id.*

252. *Id.*

253. *Id.* at 403 (majority opinion) (describing how, in exchange for the initial placement of the GPS device and once having to replace the device’s battery, the government was able to obtain more than 2,000 pages of location data over the four-week period).

254. *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018).

255. *See id.* at 2218 (“With just the click of a button, the Government can access each carrier’s deep repository of historical location information at practically no expense.”).

Using a cell-site simulator is more labor-intensive than using a GPS device or obtaining CSLI. Unlike a GPS device, a cell-site simulator does not allow law enforcement officers to passively surveil a target. In *Jones (D.C.)*, for example, officers had to drive around with a cell-site simulator in the back of their vehicle before the cell-site simulator could connect with Jones's cell phone.<sup>256</sup> Similarly, in *Lambis*, a trained DEA technician had to physically walk the cell-site simulator around an apartment complex before he was able to locate Lambis's specific apartment.<sup>257</sup>

Thus, law enforcement officers engage in active, rather than passive surveillance when they use cell-site simulators. Surveillance conducted using a cell-site simulator should not run afoul of the Fourth Amendment simply because cell-site simulators allow law enforcement officers to do their jobs more efficiently.<sup>258</sup> When law enforcement officers are engaged in active, hands-on surveillance, they are less likely to surveil a target for a prolonged period of time. This factor should also generally cut against a finding that law enforcement's use of a cell-site simulator constituted a Fourth Amendment search.

#### *D. The Nature of the Information Obtained by the Surveillance*

The fourth factor courts should consider when analyzing a cell-site simulator case is the nature of the information obtained by the cell-site simulator. If, as in *Andrews*, *Lambis*, and *Jones (D.C.)*, the information is limited to the target cell phone's "pings," then this factor should cut against a finding

---

256. See *Jones*, 168 A.3d at 708 (describing the officers driving around the area of a specified metro station with a cell-site simulator in the back of their vehicle).

257. See *Lambis*, 197 F. Supp. 3d at 609 (describing the DEA technician walking the halls of Lambis's apartment building with a cell-site simulator).

258. See *United States v. Knotts*, 460 U.S. 276, 284 (1983) ("We have never equated police efficiency with unconstitutionality, and we decline to do so now."); Richard H. McAdams, Note, *Tying Privacy in Knotts: Beeper Monitoring and Collective Fourth Amendment Rights*, 71 VA. L. REV. 297, 314 (1985) ("Individuals understand that police sometimes engage in extended visual surveillance. Our society has accepted the ancient surveillance technique of physical shadowing since the founding of our government.").

that the use of the cell-site simulator constituted a search.<sup>259</sup> When used in this way, cell-site simulators are similar to the beeper devices in *Knotts* and *Karo*.<sup>260</sup> Under *Knotts* and *Karo*, the use of cell-site simulators does not constitute a Fourth Amendment search unless the pings reveal information regarding the interior of an individual’s own home.<sup>261</sup>

The location information generated by the cell-site simulators in *Andrews*, *Lambis*, and *Jones (D.C.)* is distinguishable from the CSLI at issue in *Carpenter*. In *Carpenter*, the prosecution used Carpenter’s CSLI to generate maps placing Carpenter’s phone near the locations of four separate robberies at the date and time each robbery took place.<sup>262</sup> Unlike CSLI, cell-site simulators cannot be used to generate extensive records chronicling a target user’s past movements.<sup>263</sup> Whereas CSLI is collected and stored by wireless carriers for years, a cell-site simulator only tracks a cell phone’s location in real-time and does not store this information.<sup>264</sup> The historical nature of CSLI was essential to the *Carpenter* Court’s holding: “We do not express a view on matters not before us . . . real-time CSLI or ‘tower-dumps’ (a download of information on all the devices that connected to a particular cell site during a particular interval).”<sup>265</sup>

---

259. See, e.g., *United States v. Lambis*, 197 F. Supp. 3d 606, 609 (S.D.N.Y. 2016) (“The [cell-site simulator] then calculates the strength of the ‘pings’ until the target phone is pinpointed.”).

260. See *McAdams*, *supra* note 258, at 313–14 (explaining that beepers function like radio transmitters and therefore require “continued observation to discover someone’s identity, route, and final destination”).

261. See *supra* Part II.B.3 (discussing the interplay between the Supreme Court’s holdings in *Knotts* and *Karo*).

262. See *Carpenter*, 138 S. Ct. at 2213 (“In the Government’s view, the location records clinched the case: They confirmed that Carpenter was right where the . . . robbery was at the exact time of the robbery.” (citation omitted)).

263. See *Pell & Soghoian*, *supra* note 37, at 17 (illustrating the following uses for cell-site simulators: (1) identifying unknown phones currently used by the target, (2) locating devices, and (3) selectively blocking devices).

264. See *id.* at 24–25 (pointing out that a warrant is not needed for law enforcement’s use of digital analyzers and cell-site simulators when they are employed to intercept non-content data, such as real-time location information).

265. *Carpenter v. United States*, 138 S. Ct. 2206, 2220 (2018).



Law enforcement's uses of cell-site simulators in *Andrews*, *Lambis*, and *Jones (D.C.)* were similarly distinguishable from accessing the contents of a cell phone, which the Supreme Court has held constitutes a Fourth Amendment search.<sup>266</sup> If, as has been suggested by the EFF, law enforcement were to use a cell-site simulator to log cell phones' metadata and content,<sup>267</sup> then under *Riley v. California*,<sup>268</sup> the use of the cell-site simulator would constitute a search.<sup>269</sup> In *Riley*, the Court considered whether law enforcement may, as part of a search incident to lawful arrest,<sup>270</sup> search the digital information stored on an arrestee's cell phone without a warrant.<sup>271</sup> The Court held that law enforcement must generally obtain a search warrant before searching a cell phone and accessing its digitally stored information.<sup>272</sup>

Contrary to the holdings in *Andrews*, *Lambis*, and *Jones (D.C.)*, using a cell-site simulator does not categorically constitute a Fourth Amendment search. Courts should analyze each of the four factors discussed above to determine whether, by using a cell-site simulator, law enforcement officers engaged in a Fourth Amendment search.

---

266. See *Riley v. California*, 573 U.S. 373, 386 (2014) (holding that officers must secure a warrant before conducting a search of data on cell phones).

267. See *Cell-Site Simulators/IMSI Catchers*, *supra* note 35 ("Some cell-site simulators may have advanced features allowing law enforcement to intercept communications or even alter the content of communications.").

268. 573 U.S. 373 (2014).

269. See *id.* at 403 ("Our answer to the question of what police must do before searching [the contents of] a cell phone seized incident to an arrest is accordingly simple—get a warrant.").

270. See *id.* at 391 ("The search incident to arrest exception rests not only on the heightened government interests at stake in a volatile arrest situation, but also on an arrestee's reduced privacy interests upon being taken into police custody.").

271. See *id.* at 378 (considering the "common question" of "whether the police may, without a warrant, search digital information on a cell phone seized from an individual who has been arrested").

272. See *id.* at 386 (declining to extend the search incident to a lawful arrest exception to the warrant requirement to the digital information stored on cell phones).

*IV. A Search Does Not Violate the Fourth Amendment Unless It Is Unreasonable*

Assuming, after consideration of the four factors discussed in Part III, a court concludes that law enforcement’s use of a cell-site simulator constituted a Fourth Amendment search, the court must next determine whether the search was reasonable. The reasonableness requirement is the ultimate touchstone and “fundamental command” of the Fourth Amendment.<sup>273</sup> In drafting the Fourth Amendment, the Framers recognized that searches and seizures were “too valuable to law enforcement to prohibit them entirely,” but that “they should be slowed down.”<sup>274</sup> In determining the reasonableness of a search or seizure, courts measure both the permissibility of the initial decision to search or seize and the permissible scope of those intrusions.<sup>275</sup>

*A. Four Models for Determining Reasonableness*

Despite the importance of reasonableness to the Fourth Amendment, the Supreme Court has failed to settle on a single reasonableness standard. Professor Thomas Clancy suggests that historically, the Supreme Court has used four models to determine the reasonableness of a search or seizure: (1) the warrant preference model, (2) the individualized suspicion model, (3) the balancing model, and (4) the common law plus balancing model.<sup>276</sup>

---

273. *New Jersey v. T.L.O.*, 469 U.S. 325, 340 (1985).

274. *Berger v. New York*, 388 U.S. 41, 75 (1967) (Black, J., dissenting)

Obviously, those who wrote this Fourth Amendment knew from experience that searches and seizures were too valuable to law enforcement to prohibit them entirely, but also knew at the same time that while searches or seizures must not be stopped, they should be slowed down, and warrants should be issued only after studied caution.

275. *See Terry v. Ohio*, 392 U.S. 1, 20 (1968) (determining that the reasonableness of a search requires a twofold inquiry: first, consider “whether the . . . action was justified at its inception,” and second, determine whether the search as conducted “was reasonably related in scope to the circumstances which justified the interference in the first place”).

276. CLANCY, *supra* note 87, at 682–85.

Under the warrant preference model, “a search or seizure is not unreasonable, and therefore not forbidden, when it is carried out with a warrant issued pursuant to the criteria set out in the Warrant Clause.”<sup>277</sup> Under the individualized suspicion model, for a search or seizure to be reasonable, law enforcement must have either probable cause or reasonable suspicion, but not necessarily a warrant, prior to executing the search or seizure.<sup>278</sup> Under the balancing model, the reasonableness of a search or seizure hinges on the balancing of governmental interests against individual interests.<sup>279</sup> Under the common law plus balancing model, courts first ask “whether the action was regarded as an unlawful search or seizure under the common law when the Amendment was framed.”<sup>280</sup> Should that inquiry “yield no answer,” courts next “evaluate the search or seizure under traditional standards of reasonableness by assessing, on the one hand, the degree to which it intrudes upon an individual’s privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.”<sup>281</sup>

---

277. *Id.* at 682. Justice Frankfurter, a staunch advocate for the warrant preference model, argued that “[o]ne cannot wrench ‘unreasonable searches’ from the text, context, and historic content of the Fourth Amendment.” *United States v. Rabinowitz*, 339 U.S. 56, 69 (1950) (Frankfurter, J., dissenting).

278. *See id.* at 685 (discussing the individualized suspicion model); *see also* *Carroll v. United States*, 267 U.S. 132, 153–54 (1925) (creating the “automobile exception” and holding that a warrant is not always required, and thus is not the *sine qua non* of reasonableness).

279. *See* *Camara v. Mun. Court of S.F.*, 387 U.S. 523, 537 (1967) (balancing “the need to search against the invasion which the search entail[ed]”); *see also* *Wyoming v. Houghton*, 526 U.S. 295, 306 (1999) (noting that the “practical realities” associated with balancing competing governmental and individual interests “militate in favor of the needs of law enforcement, and against a personal-privacy interest that is ordinarily weak”).

280. *Houghton*, 526 U.S. at 299.

281. *Id.* at 300.

*B. The Warrant Preference Model Is Best-Suited to Analyzing the Reasonableness of Cell-Site Simulators*

Of the four models, the warrant preference model is best-suited to cases involving cell-site simulators. Under the warrant preference model, a search or seizure is unreasonable, and therefore unconstitutional, when carried out without a warrant issued pursuant to the criteria set out in the Warrant Clause.<sup>282</sup> Although courts no longer categorically apply the warrant preference model, the Supreme Court continues to use this model as a means of determining the reasonableness of a search or seizure, particularly in cases in the criminal law enforcement context.<sup>283</sup>

Generally, law enforcement officers use cell-site simulators in the “enterprise of ferreting out crime.”<sup>284</sup> Law enforcement’s objectives in using cell-site simulators are penal, rather than regulatory.<sup>285</sup> As such, the two reasonableness

---

282. See CLANCY, *supra* note 87, at 682 (discussing the origins of the warrant preference model); U.S. CONST. amend. IV (“[N]o warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”).

283. See *id.* at 684 (“The warrant preference model remains one of the methods the Court uses to measure reasonableness”); see also, e.g., *Katz v. United States*, 389 U.S. 347, 357 (1967) (“Searches conducted without warrants have been held unlawful ‘notwithstanding facts unquestionably showing probable cause’ . . .”); *Wong Sun v. United States*, 371 U.S. 471, 481–82 (1963) (discussing the need for the “deliberate impartial judgment of a judicial officer” to be “interposed between the citizen and the police”).

284. See *Johnson v. United States*, 333 U.S. 10, 14 (1948) (explaining that a “neutral and detached magistrate,” rather than an officer engaged in the “enterprise of ferreting out crime,” should be the one to determine “[w]hen the right of privacy must reasonably yield to the right of search”).

285. See Scott E. Sundby, *A Return to Fourth Amendment Basics: Undoing the Mischief of Camara and Terry*, 72 MINN. L. REV. 383, 408 (1988) (arguing that terms such as “administrative search” or “inspection” do not effectively limit the Supreme Court’s holding in *Camara* to administrative search cases); see also *Michigan v. Clifford*, 464 U.S. 287, 294–95 (1984) (distinguishing between administrative and conventional search warrants based on whether the objective of the search is criminal evidence); *Michigan v. Tyler*, 436 U.S. 499, 504–05 (1978) (discussing whether the government’s intent in conducting a search was administrative or criminal).

balancing models, which have been relegated to the administrative search or “community-caretaking” context, are inapplicable to law enforcement’s use of cell-site simulators.<sup>286</sup>

Should courts begin regularly applying the warrant preference model to cases involving cell-site simulators, law enforcement can “more easily predict whether their actions will be considered constitutional.”<sup>287</sup> Additionally, cell-site simulators are often used in conjunction with other surveillance technology, such as CSLI, which require law enforcement officers to obtain a search warrant.<sup>288</sup> Thus, a request to use a cell-site simulator can and should be included in law enforcement’s application for a search warrant. As with other surveillance technology, when law enforcement officers procure a search warrant, “there is little question that the subsequent search will be deemed valid.”<sup>289</sup> A general rule that a search warrant is required, qualified by necessary exceptions, will provide law enforcement officers with much-needed clarity.<sup>290</sup>

---

286. See Michael R. Diminio, Sr., *Police Paternalism: Community Caretaking, Assistance Searches, and Fourth Amendment Reasonableness*, 66 WASH. & LEE L. REV. 1485, 1487 (2009) (explaining that, when a search or seizure is undertaken for purposes other than law enforcement, the “ordinary presumption that warrantless searches are unreasonable ceases to apply”).

287. See Cynthia Lee, *Reasonableness with Teeth: The Future of Fourth Amendment Reasonableness Analysis*, 81 MISS. L.J. 1133, 1139 (2012) (“Police officers can more easily predict whether their actions will be considered constitutional under the warrant preference view than under an interpretation of the Fourth Amendment that just tells them they need to act ‘reasonably.’”).

288. See *Carpenter v. United States*, 138 S. Ct. 2206, 2221 (2018) (holding that law enforcement officers must obtain a search warrant supported by probable cause prior to accessing historic cell-site location information); see also *United States v. Lambis*, 197 F. Supp. 3d 606, 608 (S.D.N.Y. 2016) (writing that DEA agents had sought a warrant for pen register information and CSLI for Lambis’s cell phone before using the cell-site simulator).

289. Lee, *supra* note 287, at 1139.

290. See *id.* (describing the Supreme Court’s reliance on providing law enforcement officers with clear guidance); see also, e.g., *Illinois v. Lafayette*, 462 U.S. 640, 648 (1983) (stressing the importance of clear rules for inventories of arrestees); *New York v. Belton*, 453 U.S. 454, 458–60

### V. Conclusion

Electronic surveillance technology has undoubtedly come a long way since the Supreme Court's decisions in *United States v. Knotts* and *United States v. Karo*.<sup>291</sup> The cell-site simulators at issue in *Andrews*, *Lambis*, and *Jones (D.C.)* are far more sophisticated than the beepers in *Knotts* and *Karo*, or even the thermal imager in *Kyllo v. United States*.<sup>292</sup> The Supreme Court's more recent decisions in *Carpenter v. United States* and *Riley v. California* seem to indicate that cell phones and the location information they generate are entitled to special consideration under the Fourth Amendment.<sup>293</sup> Thus, it is tempting to conclude that cell-site simulators, by virtue of their sophistication, efficiency, and interaction with cell phones, categorically violate the Fourth Amendment's mandate that “the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.”<sup>294</sup> The courts in *Andrews*, *Lambis*, and *Jones (D.C.)* adopted this rationale. Taken together, their holdings indicate that any time law enforcement officers use a cell-site simulator, they conduct a search within the meaning of the Fourth Amendment.<sup>295</sup>

The courts in *Andrews*, *Lambis*, and *Jones (D.C.)* were clearly concerned about the threats to privacy that coincide with advances in surveillance technology.<sup>296</sup> While this concern

---

(1981) (emphasizing the need for “bright lines” regarding permissible scope of searches incident to lawful arrests).

291. See *supra* Part II.B.3 (discussing the beeper devices used in *Knotts* and *Karo*).

292. See *supra* Part I.B (explaining how cell-site simulators work).

293. See *Carpenter*, 138 S. Ct. at 2217 (holding that “an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI”); *Riley v. California*, 573 U.S. 373, 393 (2014) (recognizing that in light of the “immense storage capacity” of modern cell phones, police officers must generally obtain a warrant before searching the contents of a cell phone).

294. U.S. CONST. amend IV.

295. See *supra* Part III (critiquing the holdings in *Andrews*, *Lambis*, and *Jones (D.C.)*).

296. See *Kyllo v. United States*, 533 U.S. 27, 51 (2001) (Stevens, J., dissenting) (commending the Court's concern “about the threats to privacy

is commendable, in ruling on cell-site simulator cases, courts cannot “rest[] on a too-generic description of the facts” surrounding the use of the cell-site simulator.<sup>297</sup> As with any issue that implicates the Fourth Amendment, it is important to be clear about what actually occurred.<sup>298</sup> Instead of adhering to the categorical rationales utilized in *Andrews*, *Lambis*, and *Jones (D.C.)*, courts should analyze the four factors discussed in Part III to determine, on a case-by-case basis,<sup>299</sup> whether law enforcement’s use of a cell-site simulator constituted a search.<sup>300</sup> If a court concludes that the use of a cell-site simulator constituted a search, then that search should be considered unreasonable, and in violation of the Fourth Amendment, if it was conducted without a search warrant.<sup>301</sup> Broader, more comprehensive regulations regarding the use of cell-site simulators are better left to Congress and state and local legislatures.<sup>302</sup>

---

that may flow from advances in the technology available to the law enforcement profession”).

297. See *Jones v. United States*, 168 A.3d 703, 728 (D.C. Ct. App. 2017) (Thompson, J., dissenting) (arguing that, despite the commendable concern about threats to privacy that flow from advances in law enforcement technology, the court’s conclusion was based on a “too-generic description of the facts surrounding use of the cell-site simulator”).

298. See *United States v. Jones*, 565 U.S. 400, 404 (2012) (emphasizing that “[i]t is important to be clear about what occurred in this case”).

299. See Brief of Professor Orin S. Kerr as Amicus Curiae Supporting Appellant, *In re United States for Historical Cell Site Data*, 724 F.3d 600 (5th Cir. 2013) (No. 11-20884) (arguing that ex post review of law enforcement’s actions is “essential because Fourth Amendment law is extremely fact-specific” and courts “cannot apply the Fourth Amendment when no facts yet exist”).

300. See *supra* Part III (discussing the four factors: (1) whether the surveillance infringed on a constitutionally protected area, (2) the duration of the surveillance, (3) whether the surveillance was active or passive, and (4) the nature of the information obtained by the surveillance).

301. See *supra* Part IV.B (arguing that the warrant preference model of determining reasonableness should be applied to cases involving law enforcement’s use of cell-site simulators).

302. See, e.g., *DeGeer*, *supra* note 23, at 352 (arguing that Congress should draft a bill “enumerating when, how, and by whom a cell-site simulator may be used”).