

GEORGE FLOYD, GENERAL WARRANTS, AND CELL-SITE SIMULATORS

Brian L. Owsley*

ABSTRACT

The Fourth Amendment was enacted to prevent the government from utilizing general warrants. Instead, the government must obtain a warrant that is based on the specificity or particularity of the person, place, or thing to be searched. This approach evolved from a property-centric approach to safeguarding Fourth Amendment rights to one that is based on reasonable expectations of privacy.

Technology has long been a factor in law enforcement and balancing Fourth Amendment rights. As technology embeds itself in more of our lives, its constitutional impact also grows. Law enforcement periodically uses a device called a cell-site simulator to obtain personal information and data from cell phones. Essentially, a cell-site simulator works by mimicking a cell phone tower. All cell phones in a certain radius then attempt to register with the cell-site simulator for purposes of assuring that they can receive and send calls and data.

In law enforcement's gathering of data from a large number of cell phones, law enforcement essentially has a general warrant that violates the Fourth Amendment. The history of general warrants in England and in our own country demonstrates the problem of gathering this data. This Article delves into this history, focusing on notable developments in England as well as colonial America. Regardless of whether one applies a property-centric approach or a reasonable expectation of privacy analysis, cell-site simulators present problems resembling those of general warrants.

*There are reports that cell-site simulators have been used to target crowds at protest rallies in Chicago. Similarly, there were reports of such surveillance during the protests over Freddie Gray's death in Baltimore. Finally, the recent protests in the summer of 2020 over George Floyd's death have drawn a massive response by law enforcement. This Article seeks to establish that using cell-site simulators constitutes a search based on *United States v. Carpenter* as well as the handful of decisions that address cell-site simulators in state and federal*

* Associate Professor of Law, University of North Texas Dallas College of Law; B.A., University of Notre Dame, J.D., Columbia University School of Law, M.I.A., Columbia University School of International and Public Affairs. From 2005 until 2013, the author served as a United States Magistrate Judge for the United States District Court for the Southern District of Texas. The author appreciates the assistance of Dean Felecia Epps and the UNT Dallas College of Law in support of this article. Similarly, the author owes much gratitude to the 2020 SEALS Criminal Law & Criminal Procedure Workshop, including Terrence Cain, Ngov Eang, Adam Gershowitz, Nicholas Kahn-Fogel, Corinna Lain, Suparna Malempati, Jennifer Moore, and Melanie Wilson. Finally, the author wants to thank Professor Christina Masso for her amazing assistance in editing and her numerous suggestions that enhanced this article.

courts. In addition, this Article calls for solutions to the problem they pose to Fourth Amendment rights.

INTRODUCTION 151

I. THE EARLY BACKLASH AGAINST GENERAL WARRANTS 152

 A. *The English Courts Reject General Warrants* 152

 B. *The American Colonists Reject General Warrants.* 154

 C. *State Constitutions and the Fourth Amendment Reject General Warrants* 155

II. THE SUPREME COURT’S FOURTH AMENDMENT JURISPRUDENCE REJECTS GENERAL WARRANTS. 157

 A. *The Court Finds Fourth Amendment Violations Based on Physical Trespass, But Not Based on Technologically Aided Surveillance* 158

 B. *The Court Finds Fourth Amendment Violations Based on Reasonable Expectation of Privacy* 161

 C. *The Pendulum of Fourth Amendment Jurisprudence Swings Back.* 162

III. LAW ENFORCEMENT CAN USE CELL-SITE SIMULATORS TO GATHER DATA FROM CELL PHONES. 166

 A. *A Cell Phone Operates by Sending and Receiving Radio Waves to a Cell Tower, and a Cell Cite Simulator Mimics a Cell Tower to Gather Data* 166

 B. *There Are an Array of Different Cell-site Simulators with Different Features.* 169

 C. *Law Enforcement Officers Can Use Cell-site Simulators in Three Different Manners.* 171

IV. THE USE OF CELL-SITE SIMULATORS CONSTITUTES A SEARCH 173

 A. *The Supreme Court Has Not Explicitly Addressed Cell-Site Simulators, But Its Decisions Provide Some Guidance* 174

 1. *The Use of Thermal Imaging Devices Violates the Fourth Amendment* 175

 2. *Law Enforcement Must Obtain a Search Warrant in Order to Obtain Cell Site Location Information* 176

 B. *Some Courts Have Specifically Concluded a Warrant Is Required When the Police Use Cell-Site Simulators* 178

 C. *Some Courts Analyze Cell-Site Simulator Decisions Based on the Assumption that a Search Warrant is Necessary* 183

 D. *In Some Prosecutions, the Government Has Conceded That a Search Warrant Was Necessary to Use a Cell-Site Simulator* . . . 185

V. LAW ENFORCEMENT OFFICIALS’ USE OF CELL-SITE SIMULATORS TO CONDUCT MASS SURVEILLANCE VIOLATES THE FOURTH AMENDMENT AS A GENERAL WARRANT	188
A. <i>New York</i>	190
B. <i>Chicago</i>	191
C. <i>Baltimore</i>	193
CONCLUSION	194

INTRODUCTION

A general warrant gives law enforcement officers broad powers to engage in a search. In the modern parlance of the Fourth Amendment, it would be a search not defined in terms of the particularity of the person, place, or thing to be searched. The general warrant would then entitle the search officers to seize whatever they found.

If a police officer obtains a warrant to search an apartment within a twenty-unit building, that officer cannot then search all twenty apartments, but instead can only search the one authorized by the warrant. If the officer were authorized to search the entire building or an entire block, that would violate the Fourth Amendment as a general warrant.

However, if an officer obtains a search warrant authorizing the use of a cell-site simulator to locate a cell phone in that same twenty-unit building, that officer will obtain cell phone evidence from the suspect’s apartment along with the remaining nineteen apartments. The people in the other nineteen units would be the victims of overzealous surveillance within a general warrant framework. While the former circumstance is seemingly unheard of these days, the latter scenario is all too common.

Problematically, law enforcement officials have used cell-site simulators to target protestors at rallies and protests around the country. Because of the secrecy surrounding this device, usage on protestors is often only discovered long after the protests are over. There is growing evidence that police officers used cell-site simulators at protests over the killings of Eric Garner, Michael Brown, and Freddie Gray, as well as at other Black Lives Matter protests. Given this evidence, there is every reason to believe that the recent protests across the nation over the killing of George Floyd would have also attracted officers with cell-site simulators. With all of the protests that have happened since 2020 and the likelihood that more are coming, it is important to consider how cell-site simulators may be used during such protests.

Part I of this Article discusses general warrants and how people in England and America rejected their use before and up to the development of the Fourth Amendment. This disdain occurred not only in colonial America but also amongst the states as they developed their constitutions. Part II discusses the United States

Supreme Court's development of two approaches to interpreting the Fourth Amendment, both of which reject general warrants.

Next, Part III discusses what a cell-site simulator is and how it functions. Then, Part IV analyzes why the use of a cell-site simulator constitutes a search pursuant to the Fourth Amendment. Finally, Part V then addresses how cell-site simulator searches are unconstitutional general warrants. Specifically, it discusses how various protests across the country in recent years have attracted the use of cell-site simulators by law enforcement officials.

I. THE EARLY BACKLASH AGAINST GENERAL WARRANTS

In discussing general warrants, it is natural to begin with the Fourth Amendment:

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

However, the Fourth Amendment did not spring from a vast void but developed in a historical context. Similarly, prohibition of general warrants and the American aversion to them grew out of the constitutional framers' historical experience.

A. *The English Courts Reject General Warrants*

General warrants enable the government to violate the privacy of numerous citizens simultaneously. At common law, English courts issued general warrants for theft offenses, enabling law enforcement officers to engage in extremely expansive searches.² Indeed, Sir Edward Coke wrote that the Magna Carta barred justices of the peace from issuing warrants based on mere suspicions to search homes for stolen goods.³ Similarly, William Blackstone decried general warrants: "A general warrant to apprehend all persons suspected, without naming or describing any person in special, is illegal and void for its uncertainty."⁴ Eventually, English citizens began to push back on some of the abuses of the Crown's use of general warrants, and English prosecutions abandoned the use of this type of warrant. Thereafter, more information was required to obtain a warrant and engage in a search.⁵

1. U.S. CONST. amend. IV.

2. See Leonard W. Levy, *Origins of the Fourth Amendment*, 114 POL. SCI. Q. 79, 81-82 (1999); David E. Steinberg, *The Uses and Misuses of Fourth Amendment History*, 10 U. PA. J. CONST. L. 581, 600 (2008).

3. See Steinberg, *supra* note 2, at 600 (citing EDWARD COKE, *THE FOURTH PART OF THE INSTITUTES OF THE LAWS OF ENGLAND: CONCERNING THE JURISDICTION OF COURTS* 176 (London, W. Clarke & Sons 1817) (1644)).

4. Steinberg, *supra* note 2, at 600 n.105.

5. See Jeanne N. Lobelson, *The Warrant Clause*, 26 AM. CRIM. L. REV. 1433, 1436-37 (1989); see, e.g., Steinberg, *supra* note 2, at 600-01 (citing precedent from the English courts which concluded that overbroad searches of homes violated English common law principles.).

The use of general warrants in England became intertwined with press freedoms.⁶ Particularly problematic was the Secretary of State's use of general warrants to search citizens' homes for books and papers to develop charges of libel against the homeowners.⁷

The first notable case, *Wilkes v. Wood*,⁸ concerned John Wilkes's anonymous publication of *The North Briton*, a radical newspaper.⁹ In issue number forty-five, Wilkes, an opposition member of the House of Commons, criticized King George III for entering into a peace treaty with France that was too favorable to the French.¹⁰ Moreover, the newspaper characterized "the British Tory administration as 'wretched puppets,' . . . and 'the tools of corruption and despotism.'"¹¹

In response to this periodical, Lord Halifax, the Secretary of State, sent the King's Messengers to search all printers and publishers for evidence of this newspaper.¹² As one prominent historian explained, "Crown agents enforcing the warrants had unfettered discretion to search, seize, and arrest anyone as they pleased."¹³ The King's Messengers seized Wilkes' private papers as well as books and papers of individuals associated with him.¹⁴ Based on this volume of seized material, the House of Commons determined that the publication constituted seditious libel and expelled him.¹⁵

Wilkes filed a trespass action in the English Court of Common Pleas. The judge criticized the warrant as an attack on all of England, awarding Wilkes damages in his action against Wood, one of the King's Messengers, in the amount of 1,000 pounds and against Lord Halifax because he issued the warrant in the amount of 4,000 pounds.¹⁶

Several years later, an even more influential case was decided by the British courts: *Entick v. Carrington*.¹⁷ Lord Halifax again issued a warrant authorizing four King's Messengers to search John Entick's home for seditious materials related to Entick's publication of the *Monitor* or the *British Freeholder*.¹⁸ Over a period of about four hours, these four individuals searched Entick's home, broke

6. See *Marcus v. Search Warrants of Prop.* at 104 E. Tenth St., Kan. City, 367 U.S. 717, 724–25 (1961).

7. See *Boyd v. United States*, 116 U.S. 616, 625–26 (1886).

8. 98 Eng. Rep. 489 (K.B. 1763).

9. See *id.* at 493–94.

10. See *Boyd*, 116 U.S. at 625–26.

11. Steinberg, *supra* note 2, at 601 (internal quotations omitted).

12. See *Wilkes*, 98 Eng. Rep. at 494, 496; see also *Stanford v. Texas*, 379 U.S. 476, 483 (1965) (citing NELSON B. LASSON, HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION 48 (1970)).

13. Levy, *supra* note 2, at 86.

14. See *id.*

15. See *id.*

16. See *Wilkes*, 98 Eng. Rep. at 499; *Boyd*, 116 U.S. at 626.

17. 19 How. St. Tr. 1029 (K.B. 1765).

18. See *Entick*, 19 How. St. Tr. at 1030–31; see also *Stanford*, 379 U.S. at 483 ("A warrant was issued specifically naming him and that publication, and authorizing his arrest for seditious libel and the seizure of his 'books and papers.'").

open locked boxes, and scoured through his possessions.¹⁹ When they finished, they carried away about 100 pamphlets and 100 charts.²⁰

Entick sued the four King's Messengers in the Court of Common Pleas pursuant to a claim in trespass.²¹ Presiding as Chief Justice, Lord Camden found that the warrant issued by Lord Halifax violated the law as an invasion of the home:

This power so assumed by the secretary of state is an execution upon all the party's papers, in the first instance. His house is rifled; his most valuable secrets are taken out of his possession, before the paper for which he is charged is found to be criminal by any competent jurisdiction, and before he is convicted either of writing, publishing, or being concerned in the paper.²²

Furthermore, he rejected Lord Halifax's argument that he had the power to issue such general warrants, concluding that such a power would be too extreme: "Such is the power, and therefore one would naturally expect that the law to warrant it should be clear in proportion as the power is exorbitant. If it is law, it will be found in our books; if it is not to be found there it is not law."²³ After Lord Camden's decision in *Entick*, the British House of Commons issued two resolutions condemning general warrants, most notably condemning their use in libel investigations.²⁴

B. The American Colonists Reject General Warrants

In 1761, on the other side of the pond, Massachusetts attorney James Otis, Jr. represented a number of colonial merchants in the Writs of Assistance Case.²⁵ New writs of assistance were being proposed to replace the old ones that lapsed in 1760 with the death of King George II.²⁶ Charles Paxton was a customs officer in Boston who sought a new writ of assistance from the Superior Court in 1761 following the king's death.²⁷ Massachusetts colonial courts issued writs of assistance in response to colonists' attempts to avoid paying customs duties on imported goods. Writs of assistance allowed customs officials to basically search anywhere for anything related to smuggling that violated the customs laws.²⁸ Indeed, the

19. See *Entick*, 19 How. St. Tr. at 1030; see also *Stanford*, 379 U.S. at 483–84 ("The King's messengers executing the warrant ransacked Entick's home for four hours and carted quantities of his books and papers away.").

20. See *Entick*, 19 How. St. Tr. at 1030.

21. See *id.* at 1029.

22. See *id.* at 1064; see also *Marcus v. Search Warrants of Prop.* at 104 E. Tenth St., Kan. City, 367 U.S. 717, 728 (quoting *Entick*, 19 How. St. Tr. at 1064).

23. *Boyd*, 116 U.S. at 627 (quoting *Entick*, 19 How. St. Tr. at 1065–66).

24. See *Stanford*, 379 U.S. at 484; *Boyd*, 116 U.S. at 625.

25. See Thomas K. Clancy, *The Fourth Amendment's Concept of Reasonableness*, 2004 UTAH L. REV. 977, 982–84 (2004); Levy, *supra* note 2, at 84.

26. See Tracey Maclin, *The Complexity of the Fourth Amendment: A Historical Review*, 77 B.U. L. REV. 925, 946–47 (1997); Levy, *supra* note 2, at 84.

27. See David E. Steinberg, *An Original Misunderstanding: Akhil Amar and Fourth Amendment History*, 42 SAN DIEGO L. REV. 227, 260 (2005).

28. See *Boyd*, 116 U.S. at 625.

writs of assistance were much broader than the English general warrants in the libel cases because they authorized seizures of any illegal imported merchandise and had no limit on the duration or location of the search.²⁹

Otis argued that the requested writs of assistance were general warrants and that allowing writs of assistance would weaken the privacy of every homeowner.³⁰ He reiterated the notion developed in English jurisprudence by Lord Camden, that one's home is one's castle.³¹ Forcefully, Otis asserted that writs of assistance are "the worst instrument of arbitrary power, the most destructive of English liberty and the fundamental principles of law, that ever was found in an English law-book."³² He further maintained that special writs should be "granted on oath and probable suspicion [A]n officer should show probable grounds, should take his oath on it, should do this before a magistrate, and . . . such magistrate, if he thinks proper should issue a special warrant to a constable to search the places."³³ In other words, Otis proposed that warrants should contain a location, a given suspected offense, and the person alleging the criminal conduct. Ultimately, the Superior Court granted Paxton his use of the writ of assistance.³⁴

Although Otis lost this case, his argument greatly influenced John Adams, who characterized Otis's oratory as one of the first strikes of the American Revolution: "[T]hen and there was the first scene of the first act of opposition to the arbitrary claims of Great Britain. Then and there the child Independence was born."³⁵ Indeed, Adams noted that Otis argued general warrants were no longer favored for one's home, and that special warrants were required instead.

C. State Constitutions and the Fourth Amendment Reject General Warrants

As colonial leaders began to push for individual rights from the British monarchy, if not for independence, they began to voice opposition to general warrants. In 1776, George Mason was the primary drafter of the Virginia Declaration of Rights, including Section 10,³⁶ which provided that:

[G]eneral warrants, whereby an officer or messenger may be commanded to search suspected places without evidence of a fact committed, or to seize any person or persons not named, or whose offense is not particularly described and supported by evidence, are grievous and oppressive and ought not to be granted.³⁷

29. See *Marcus v. Search Warrants of Prop.* at 104 E. Tenth St., Kan. City 367 U.S. 717, 729 n.22 (1961).

30. See Clancy, *supra* note 25, at 982–84.

31. See *id.*

32. James Otis, *Against Writs of Assistance*, (Feb. 1761), <http://www.nhinet.org/ccs/docs/writs.htm>.

33. M.H. SMITH, *THE WRITS OF ASSISTANCE CASE* 369 (1978).

34. See Steinberg, *supra* note 27, at 261; Maclin, *supra* note 26, at 946–47.

35. *Stanford v. Texas*, 379 U.S. 476, 481–82 (1965) (quoting *Boyd v. United States*, 116 U.S. 616, 625 (1886)).

36. See Jack Wade Nowlin, *The Judicial Restraint Amendment: Populist Constitutional Reform in the Spirit of the Bill of Rights*, 78 NOTRE DAME L. REV. 171, 213 (2002).

37. VIRGINIA DECLARATION OF RIGHTS § 10 (1776).

On June 12, 1776, the Virginia Convention of Delegates unanimously adopted this section less than a month before the signing of the Declaration of Independence.³⁸

The people of Pennsylvania fashioned a similar declaration, Section X, against general searches:

That the people have a right to hold themselves, their houses, papers, and possessions free from search and seizure, and therefore warrants without oaths or affirmations first made, affording a sufficient foundation for them, and whereby any officer or messenger may be commanded or required to search suspected places, or to seize any person or persons, his or their property, not particularly described, are contrary to that right, and ought not to be granted.³⁹

On September 28, 1776, a constitutional convention ratified the Constitution of Pennsylvania, which included Section X in a Declaration of Rights of the inhabitants of the Commonwealth of Pennsylvania.⁴⁰

Otis's oratory at the proceedings in the Writs of Assistance Case inspired Adams when, in 1779, he co-authored the Massachusetts Declaration of Rights, which was adopted in 1780.⁴¹ Article 14 of the Massachusetts Declaration of Rights mandates that:

Every subject has a right to be secure from all unreasonable searches and seizures of his person, his houses, his papers, and all his possessions. All warrants, therefore, are contrary to this right, if the cause or foundation of them be not previously supported by oath or affirmation, and if the order in the warrant to a civil officer, to make search in suspected places, or to arrest one or more suspected persons, or to seize their property, be not accompanied with a special designation of the person or objects of search, arrest, or seizure; and no warrant ought to be issued but in cases, and with the formalities prescribed by the laws.⁴²

In drafting the Federal Bill of Rights, both English and colonial history influenced James Madison: "The Bill of Rights was fashioned against the background of knowledge that unrestricted power of search and seizure could also be an instrument for stifling liberty of expression."⁴³ Moreover, both Article XIV of the

38. See Nowlin, *supra* note 36, at 213; Robert J. Reinstein, *Completing the Constitution: The Declaration of Independence, Bill of Rights and Fourteenth Amendment*, 66 TEMP. L. REV. 361, 370 (1993).

39. PENNSYLVANIA DECLARATION OF RIGHTS § X (1776).

40. See Horst Dippel, *Human Rights in America, 1776–1849: Rediscovering the States' Contribution*, 67 ALB. L. REV. 713, 721 (2004).

41. See Levy, *supra* note 2, at 85 ("Adams's reaction to Otis's speech is so important because a straight line of progression runs from Otis's argument in 1761 to Adams's framing of Article XIV of the Massachusetts Declaration of Rights of 1780 to James Madison's introduction of the proposal that became the Fourth Amendment."); see also Thomas K. Clancy, *The Framers' Intent: John Adams, His Era, and the Fourth Amendment*, 86 IND. L.J. 979, 980–81 (2011).

42. Clancy, *supra* note 41, at 1028 (quoting MASS. DECLARATION OF RIGHTS Art. 14 (1780)).

43. *Marcus v. Search Warrants of Prop.* at 104 E. Tenth St., Kan. City, 367 U.S. 717, 729 (1961).

Massachusetts Declaration of Rights, as well as the Virginia Declaration of Rights, greatly influenced him.⁴⁴

The Fourth Amendment, as drafted by Madison, established a particularity requirement. Thus, a warrant is invalid pursuant to the Fourth Amendment when the warrant fails to adequately describe the person, place, or thing to be searched or seized.⁴⁵ The Supreme Court has explained that “[t]he requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another.”⁴⁶ Ultimately, law enforcement officers do not have any discretion as to what things can be taken pursuant to a warrant, but instead must simply take what is actually described.⁴⁷

II. THE SUPREME COURT’S FOURTH AMENDMENT JURISPRUDENCE REJECTS GENERAL WARRANTS

Historically, there was little in the way of Fourth Amendment jurisprudence from the Supreme Court for almost the first one hundred years because state courts handled most criminal prosecutions, as most offenses were state crimes.⁴⁸ The Bill of Rights was not interpreted to apply to the states at first.⁴⁹ In part because most criminal offenses were based on state jurisdiction, the Supreme Court did not first interpret the Fourth Amendment until 1877.⁵⁰ The Court eventually applied Fourth Amendment protections to state criminal defendants.⁵¹

Over time, the Court developed two principal ways to interpret the Fourth Amendment. Initially, the Court interpreted the Fourth Amendment based on a

44. See Clancy, *supra* note 41, at 1046 (discussing the VIRGINIA DECLARATION OF RIGHTS).

45. See also *Stanford v. Texas*, 379 U.S. 476, 485 (1965) (emphasizing that particularity requirement must be “accorded the most scrupulous exactitude” when warrants authorize seizure of particular books); see generally *Groh v. Ramirez*, 540 U.S. 551, 557 (2004).

46. *Stanford*, 379 U.S. at 485 (quoting *Marron v. United States*, 275 U.S. 192, 196).

47. *Id.*

48. Prior to 1900, two Supreme Court cases analyzed the Fourth Amendment: *Boyd v. United States*, 116 U.S. 616 (1886) and *Ex parte Jackson*, 96 U.S. 727 (1877).

49. See *Wolf v. Colorado*, 338 U.S. 25 (1949). The Court stated:

Unlike the specific requirements and restrictions placed by the Bill of Rights (Amendments I to VIII) upon the administration of criminal justice by federal authority, the Fourteenth Amendment did not subject criminal justice in the States to specific limitations. The notion that the “due process of law” guaranteed by the Fourteenth Amendment is shorthand for the first eight amendments of the Constitution and thereby incorporates them has been rejected by this Court again and again, after impressive consideration. (citations omitted).

Id. at 26.

50. See *Ex parte Jackson*, 96 U.S. 727 (1877); Adam Samaha, *Originalism’s Expiration Date*, 30 CARDOZO L. REV 1295, 1324 n.100 (2008).

51. See *Mapp v. Ohio*, 367 U.S. 643, 655 (1961) (“Since the Fourth Amendment’s right of privacy has been declared enforceable against the States through the Due Process Clause of the Fourteenth, it is enforceable against them by the same sanction of exclusion as is used against the Federal Government.”); *Stanford*, 379 U.S. at 481 (“It is now settled that the fundamental protections of the Fourth Amendment are guaranteed by the Fourteenth Amendment against invasion by the States.”) (citations omitted).

property-centric approach, meaning that a violation occurred when there was a trespass—a physical invasion—of a person’s physical property or personal objects. In 1967, the Supreme Court altered its jurisprudence with the reasonable expectation of privacy approach. Thus, a two-prong test must be met to establish a violation. First, a person must demonstrate an actual expectation of privacy, which is a subjective standard. Second, the expectation must be one that society is prepared to recognize as reasonable, which is an objective standard. Eventually, the trespass approach, which fell into disfavor, was reinvigorated such that either approach is a viable means for demonstrating a Fourth Amendment violation. Because of the historical disdain by the Framers as well as the development of Fourth Amendment jurisprudence, neither approach allows general warrants.

*A. The Court Finds Fourth Amendment Violations Based on Physical Trespass,
But Not Based on Technologically Aided Surveillance*

In *Boyd*, one of the seminal cases in the Fourth Amendment’s first century, the Supreme Court applied the concept of trespass to find a constitutional violation. The Government seized thirty-five cases of plate glass as they entered the Port of New York, alleging that the claimants failed to pay customs on these imports.⁵² The claimants argued that the Government improperly seized the cases of glass.⁵³ In advance of trial, the Government petitioned the trial court for an order requiring the claimants to produce invoices for twenty-nine other cases of glass.⁵⁴ The claimants objected to the order but provided the invoice to the Government.⁵⁵ At trial, the invoice was admitted into evidence over the claimants’ objection.⁵⁶ Ultimately, a jury found that the seizure of a total of thirty-five cases was valid, and the court entered judgment of forfeiture in the Government’s favor.⁵⁷

Per the Supreme Court, *Boyd* presented “a very grave question of constitutional law.”⁵⁸ Specifically, it addressed the issue of whether the seizure of these private papers constituted “an ‘unreasonable search and seizure’ within the meaning of the fourth amendment.”⁵⁹ In analyzing the Fourth Amendment issue, the Court noted that American notions of trespass and the Fourth Amendment are rooted in the English legal tradition.⁶⁰ Justice Bradley explored *Entick v. Carrington*, noting that it was in an action for trespass that Lord Camden had established a legal principle that resounded in both the Old and the New World. The law enforcement

52. See *Boyd v. United States*, 116 U.S. 616, 617–18 (1886).

53. See *id.* at 618.

54. See *id.*

55. See *id.*

56. See *id.*

57. See *id.*

58. *Id.*

59. *Id.* at 622.

60. See *id.* at 627.

officers violated the Fourth Amendment when they committed a trespass by seizing Boyd's private papers.⁶¹

The influence of trespass in Fourth Amendment jurisprudence continued for almost another one hundred years after *Boyd*. During the Prohibition era, federal agents suspected Roy Olmstead of running a bootlegger operation in Seattle.⁶² Consequently, some agents installed wiretaps in the basement of Olmstead's office building on the three different telephone lines to his office, as well as wiretaps on a line near his home.⁶³ There were numerous incriminating calls to Vancouver.⁶⁴ A jury convicted Olmstead based on evidence obtained from these wiretaps.⁶⁵

In a case of first impression, Olmstead challenged the evidence from these wiretaps, arguing that they violated the Fourth Amendment. Chief Justice William Howard Taft, writing for the majority, rejected this argument, finding that the Government did not infringe upon Olmstead's Fourth Amendment rights because the wiretapping was not a search and seizure within the Fourth Amendment's meaning.⁶⁶ Specifically, the Court concluded that the Fourth Amendment's language refers to actual physical examinations of one's person, papers, tangible material effects, or home but not their conversations.⁶⁷ In other words, the federal agents did not commit a trespass on any property controlled by Olmstead.

Similarly, in *Goldman v. United States*,⁶⁸ the Court addressed a federal criminal investigation concerning fraud by attorneys in a bankruptcy proceeding. Federal agents went to one of the attorney's office buildings and gained access to an adjacent office.⁶⁹ At night, with the building superintendent's cooperation, the agents "installed a small aperture in the partition wall, with a wire to be attached to earphones extending into the adjoining office" so that they could listen to a meeting with the attorneys the next day.⁷⁰

The next day, the listening aperture did not work when the federal agents attempted to use it.⁷¹ The agents had a second device—a detectaphone—that enabled them to listen to the conversation in the adjacent office with a receiver that picked up sound waves from the attorney's office and amplified them.⁷² Using the detectaphone, agents listened to the conversation among the people in the

61. *See id.* at 627–28.

62. *Olmstead v. United States*, 277 U.S. 438, 455–56 (1928).

63. *See id.* at 456–57.

64. *See id.* at 456.

65. *See id.* at 455–56.

66. *See id.* at 464–66.

67. *See id.* at 465–66.

68. 316 U.S. 129 (1942).

69. *See id.* at 131.

70. *Id.*

71. *See id.*

72. *See id.*

attorney's office. Additionally, a stenographer transcribed parts of the conversation, which in turn the Government used to prosecute the attorneys.⁷³

The petitioners argued before the Supreme Court that the installation of the first listening device into the partition wall constituted a trespass.⁷⁴ Moreover, they maintained that the trespass facilitated the placement and use of the detectaphone when the listening device failed to function properly.⁷⁵ While acknowledging that the first listening device constituted a trespass, the Court determined that this "trespass did not aid materially in the use of the detectaphone."⁷⁶

Next, the *Goldman* Court held that the agents' use of the detectaphone did not violate the Fourth Amendment. First, the Court rejected the petitioners' argument that these circumstances are distinguishable from *Olmstead*.⁷⁷ Second, the Court declined the petitioners' request to overrule *Olmstead*.⁷⁸ Ultimately, the Court concluded that this second device did not constitute a trespass into the attorney's office, affirming the convictions.

With the Supreme Court's Fourth Amendment jurisprudence grounded in the property-centric trespass approach, throughout the mid-twentieth century, it did not consider electronically-aided surveillance to violate the Fourth Amendment unless there was a physical intrusion. Even when there was a basis for a search consistent with notions of trespass, the government still could not exercise a general warrant. In *Boyd*, the Court first enunciated the history that the Court would echo decrying the use of general warrants: "[I]t is only *unreasonable* searches and seizures that are forbidden, and the means of securing this protection was by abolishing searches under warrants, which were called general warrants, because they authorized searches in any place, for any thing."⁷⁹ Thus, the Court determined the trespass in *Boyd* was a Fourth Amendment violation because it was a general warrant. Even though Chief Justice Taft found that the search did not violate the Fourth

73. See *id.* at 131–32.

74. See *id.* at 134. Indeed, if the Government's case had rested on evidence from the installation and use of the listening aperture, the Court likely would have found a trespass and thus a Fourth Amendment violation. In *Silverman v. United States* the Supreme Court analyzed the use of an eavesdropping that happened "by means of an unauthorized physical penetration into the premises occupied by the petitioners." 365 U.S. 505, 509 (1961). Specifically, the agents inserted a microphone on a foot-long spike through a wall and into the heating duct in Silverman's home whereby the agents could easily hear the conversations in the home. *Id.* at 506–07. The *Silverman* Court noted that the finding of a Fourth Amendment violation was not based on "the technicality of a trespass upon a party wall as a matter of local law," but instead hinged on "the reality of an actual intrusion into a constitutionally protected area." *Id.* at 512.

75. See *Goldman*, 316 U.S. at 134–35.

76. *Id.* at 135. Similarly, in *On Lee v. United States* the Supreme Court determined that a federal agent did not violate the Fourth Amendment when he electronically recorded a conversation between Lee and himself in Lee's place of business because "no trespass was committed," as the agent only recorded in a location accessible to the public. 343 U.S. 747, 751 (1952).

77. See *Goldman*, 316 U.S. at 135.

78. See *id.* at 135–36. In dissent, Chief Justice Harlan Fiske Stone and Justice Felix Frankfurter advocated that the Court should overrule *Olmstead*. *Id.* at 136 (Stone, C.J., and Frankfurter, J., dissenting).

79. *Boyd v. United States*, 116 U.S. 616, 641 (1886).

Amendment in *Olmstead*, he did so through the prism of *Boyd* and the history of general warrants.⁸⁰

B. The Court Finds Fourth Amendment Violations Based on Reasonable Expectation of Privacy

The application of the trespass doctrine to analyze Fourth Amendment violations fell into disfavor with *Katz v. United States*.⁸¹ Katz made calls from a public telephone booth to transmit betting information from Los Angeles to Boston and Miami in violation of federal law.⁸² Based on FBI surveillance, some agents attached a listening device to the booth's top, recording his side of the telephone conversations.⁸³ The Government then used Katz's words at trial to convict him.

In *Katz*, the Supreme Court addressed whether the Fourth Amendment protected the recording of private conversations in a public telephone booth. Katz argued that the phone booth was a constitutionally protected area.⁸⁴ The Government responded that its surveillance was not a trespass, relying on *Olmstead* and *Goldman*.⁸⁵

Although Katz did not try to hide from public view when he entered the telephone booth, he wanted to keep others from listening to his conversation. Justice Stewart determined that Katz did not relinquish his right to prevent others from listening simply because he went to a place where he could be seen in public: "One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world."⁸⁶ Consequently, a person who enters a telephone booth to make a call may expect Fourth Amendment protections based on the assumption that the person's words will not be accessible to anyone but the intended recipient. Thus, the Fourth Amendment protects *persons*, and not locations, from *unreasonable* searches and seizures.⁸⁷ The Court held that the Government's activities in electronically listening to and recording Katz's telephone conversations constituted a search and seizure of Katz and his person pursuant to the Fourth Amendment. Unless the Government had a search warrant based upon sufficient probable cause, all evidence obtained from that conversation was inadmissible.

This decision was an excellent outcome for Katz. However, the lasting legacy came not from Justice Stewart's majority decision but from Justice John Marshall

80. See *Olmstead v. United States*, 277 U.S. 438, 463; accord *Goldman*, 316 U.S. at 139 n.5 (Murphy, J., dissenting).

81. See 389 U.S. 347 (1967).

82. See *id.* at 348.

83. See *id.*

84. See *id.* at 349–50.

85. See *id.* at 352–53.

86. *Id.* at 352.

87. See *id.* at 353.

Harlan's concurring opinion, which embodies the principle for which the decision is known today. Justice Harlan created a two-factor requirement for what Fourth Amendment protections exist in a given situation.⁸⁸ First, a person must demonstrate an actual expectation of privacy. This factor is based on the person's subjective belief. Second, the expectation must be one that society is prepared to recognize as reasonable. This factor is based on objective determinations within society.

Applying this two-factor test, Justice Harlan found that Katz entered the telephone booth, closed the door behind him, paid for his call, and thus was reasonably entitled to believe that his conversation was not being recorded.⁸⁹ In other words, he had a subjective belief that his conduct was private. Moreover, Justice Harlan further concluded that privacy within the confines of a telephone booth was an expectation that society would recognize as reasonable.⁹⁰

After *Katz*, the new analytical approach toward assessing Fourth Amendment violations was based on the concept of whether one had a reasonable expectation of privacy in any given circumstance. The trespass approach lay moribund if not firmly dead: "We have recognized that the principal object of the Fourth Amendment is the protection of privacy rather than property, and have increasingly discarded fictional and procedural barriers rested on property concepts."⁹¹ Indeed, the *Katz* Court overruled both *Olmstead* and *Goldman*, finding that their reasoning was no longer compelling.⁹² Thus, the Supreme Court struck a significant blow against trespass as a Fourth Amendment theory in favor of reasonable expectation of privacy.

C. The Pendulum of Fourth Amendment Jurisprudence Swings Back

In 2012, Justice Antonin Scalia sought to revive the trespass theory of the Fourth Amendment. In *United States v. Jones*,⁹³ he succeeded. In *Jones*, Antoine

88. See *id.* at 361 (Harlan, J., concurring). The Supreme Court fully adopted this two-prong test in *Smith v. Maryland*, 442 U.S. 735, 740 (1979).

89. See *Katz*, 389 U.S. at 361.

90. See *id.*

91. *Warden v. Hayden*, 387 U.S. 294, 304 (1967) (citations omitted); see Brian L. Owsley, *Cell Phone Tracking in the Era of United States v. Jones and California v. Riley*, 48 TEX. TECH L. REV. 207, 210 (2015).

92. The *Katz* Court stated as follows:

We conclude that the underpinnings of *Olmstead* and *Goldman* have been so eroded by our subsequent decisions that the 'trespass' doctrine there enunciated can no longer be regarded as controlling. The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment. The fact that the electronic device employed to achieve that end did not happen to penetrate the wall of the booth can have no constitutional significance."

See *Katz*, 389 U.S. at 353; see also *id.* at 362 (Harlan, J., concurring) (rejecting *Goldman*).

93. 565 U.S. 400 (2012).

Jones owned and operated a nightclub in the District of Columbia.⁹⁴ Local police officers and the FBI suspected he engaged in the trafficking of narcotics.⁹⁵ Based on information gathered through various investigative techniques, police obtained a warrant authorizing the use of a GPS tracking device on a Grand Jeep Cherokee registered to Jones's wife (of which Jones was the exclusive driver).⁹⁶ However, in placing the tracking device on the Jeep, the police failed to comply with the warrant's mandates. Specifically, the magistrate judge authorized the warrant but required the police to put the device on the Jeep *within ten days and in the District of Columbia*.⁹⁷ Instead, the officers installed the device on the undercarriage of the Jeep *on the eleventh day in Maryland* and used it to track the vehicle's movements.⁹⁸

By satellite, the tracking device narrowed the Jeep's location within fifty to one hundred feet and communicated the location by cell phone to a government computer, relaying more than 2,000 pages of data over a twenty-eight-day period.⁹⁹ The Government ultimately obtained an indictment against Jones, which included charges of conspiracy to distribute cocaine.¹⁰⁰

In *Jones*, the Supreme Court addressed whether the attachment of a GPS tracking device to Jones's Jeep constituted a search within the meaning of the Fourth Amendment.¹⁰¹ The Court unanimously found that Jones suffered a Fourth Amendment violation based on this search even though the Justices reached this unanimity via two different paths.

Writing for a plurality including Chief Justice Roberts, Justice Kennedy, and Justice Thomas, Justice Scalia posited that the Government's physical intrusion on Jones's Jeep, which was a personal "effect," was clearly a search within the Fourth Amendment's original meaning.¹⁰² In its analysis of the Fourth Amendment, the Court was historically concerned with governmental trespass on private property for the purpose of finding something or obtaining information.¹⁰³ The *Katz* "reasonable expectation of privacy" standard did not repudiate that understanding of trespass and the Fourth Amendment but rather added to it.¹⁰⁴ In *Jones*, Justice Scalia revitalized the physical trespass approach best known from *Olmstead* that at one point had seemingly been overruled after *Katz*.¹⁰⁵

94. *See id.* at 402.

95. *See id.*

96. *See id.* at 402, 404 n.2.

97. *See id.* at 402–03 (emphases added).

98. *See id.* at 403 (emphasis added).

99. *See id.*; Owsley, *supra* note 91, at 209.

100. *See Jones*, 565 U.S. at 403; Owsley, *supra* note 91, at 209.

101. *See Jones*, 565 U.S. at 402.

102. *See id.* at 404.

103. *See Olmstead v. United States*, 277 U.S. 438, 463 (1928); *see also Kyllo v. United States*, 533 U.S. 27, 31 (2001).

104. *See Jones*, 565 U.S. at 405–09; Owsley, *supra* note 91, at 211.

105. In *Arizona v. Hicks*, 480 U.S. 321 (1987), Justice Scalia authored a decision that predicted his approach to the Fourth Amendment based on trespass. In *Hicks*, the police were investigating a shooting that came from

Justice Samuel Alito, joined by as Justices Ginsburg, Breyer, and Kagan, concurred in the judgment. However, they disagreed with the majority that any technical trespass that results in the gathering of evidence amounts to a search. Instead, they would have analyzed the case pursuant to the *Katz* standard.¹⁰⁶ Because GPS technology is relatively cheap and easy to use, it overcomes traditional practical constraints on close surveillance.¹⁰⁷ While Justice Alito deemed relatively short-term monitoring of an individual's movements on public streets reasonable under the Fourth Amendment, he argued that "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."¹⁰⁸ Here, use of GPS monitoring violated societal expectations that law enforcement would not and could not monitor all of an individual's movements in one's car for a four-week period.

Justice Sonia Sotomayor concurred, agreeing with Justice Scalia that *Katz* supplemented rather than substituted the trespassory test for whether a search has occurred.¹⁰⁹ However, she also agreed with Justice Alito that most long-term GPS monitoring would violate *Katz*, and noted that even short-term GPS monitoring may violate an individual's reasonable expectation of privacy because of the unique nature of GPS surveillance.¹¹⁰

In *Florida v. Jardines*, Justice Scalia once again bolstered his efforts to reinvigorate the trespass approach in addressing Fourth Amendment violations.¹¹¹ In November 2006, Miami police received an anonymous unverified tip through its "crime stoppers" tipline that Jardines used his residence to grow marijuana.¹¹² About a month later, two detectives and Franky, a drug sniffing dog, approached the house in the morning while other officers, along with DEA agents, established perimeter positions around the residence.¹¹³

Detective William Pedraja observed Jardines' house for fifteen minutes.¹¹⁴ There were no vehicles in the driveway, the blinds were closed, and there was no

the suspect's apartment into the one below it. *Id.* at 323. While in the apartment, one officer saw some expensive stereo equipment and picked it up to look at the serial number underneath the equipment. *Id.* Subsequently, it was determined based on the serial numbers that the equipment was indeed stolen. *Id.* The Court held that the stereo equipment was not immediately incriminating because probable cause was acquired only after an additional search. Specifically, the police officer had to lift up the stereo equipment and turn over it to get the serial numbers. Physically trespassing on someone's private property may not be a search in *Oliver v. United States*, 466 U.S. 170 (1984), and *United States v. Dunn*, 480 U.S. 294 (1987), but handling and turning over a piece of stereo equipment constituted a search.

106. See *Jones*, 565 U.S. at 422–24 (Alito, J., concurring).

107. See *id.* at 428–30 (Alito, J., concurring).

108. *Id.* at 430 (Alito, J., concurring).

109. See *id.* at 414 (Sotomayor, J., concurring).

110. See *id.* at 415 (Sotomayor, J., concurring); Owsley, *supra* note 92, at 212.

111. 569 U.S. 1 (2013).

112. See *Jardines v. State*, 73 So. 3d 34, 37 (Fla. 2011); *Jardines*, 569 U.S. 1 at 3; Brian L. Owsley, *The Supreme Court Goes to the Dogs: Reconciling Florida v. Harris and Florida v. Jardines*, 77 ALB. L. REV. 349, 367 (2013–2014).

113. See *Jardines*, 569 U.S. at 3–4; *Jardines*, 73 So. 3d at 37.

114. See *Jardines*, 569 U.S. at 3.

observable activity.¹¹⁵ After this fifteen minutes of surveillance, Detective Douglas Bartlett, a dog handler, approached the residence with the drug sniffing dog.¹¹⁶ Detective Bartlett put the dog on a leash and accompanied it to the front door, where it alerted.¹¹⁷ Detective Bartlett told Detective Pedraja that the dog had exhibited a positive alert for narcotics.¹¹⁸ On the basis of the drug dog's positive alert for narcotics at the house, Detective Pedraja then sought and obtained a search warrant for Jardines' home.¹¹⁹ The search established that Jardines grew marijuana inside his home.¹²⁰

The Florida Supreme Court granted Jardines' petition for discretionary review to address whether the use of the drug dog on his porch constituted a search pursuant to the Fourth Amendment and what standard applied to such a search.¹²¹ Ultimately, the court determined that the use of the drug dog on the porch was a search, and that the search lacked the requisite probable cause.¹²² In *Jardines*, the United States Supreme Court then addressed whether law enforcement needs probable cause and a warrant to bring a trained drug sniffing dog to a person's front door.¹²³

As in *Jones*, Justice Scalia analyzed the issue through the prism of trespass theory: "though *Katz* may add to the baseline, it does not subtract anything from the Amendment's protections 'when the Government *does* not engage in [a] physical intrusion of a constitutionally protected area.'"¹²⁴ He wrote that a home's front porch is part of the home itself for Fourth Amendment purposes based in part on notions of curtilage.¹²⁵ Typically, ordinary citizens are invited to enter onto the porch or up to the front door, either explicitly or implicitly, to communicate with the home's residents.¹²⁶ "Thus, a police officer not armed with a warrant may approach a home and knock, precisely because that is 'no more than any private citizen might do.'"¹²⁷ However, a police officer cannot go beyond the scope of that invitation. Entering a person's porch for the purposes of conducting a search

115. *See id.*

116. *See id.* at 3–4.

117. *See id.* at 4.

118. *See id.*

119. *See id.*

120. *See id.*; *Jardines v. State*, 73 So. 3d 34, 38 (Fla. 2011).

121. *See Jardines v. State*, No. SC08-2101, 2009 WL 424721 (Fla. Feb. 4, 2009); *Jardines*, 73 So. 3d at 35; *see also* Stephen A. Simon, *Dog Sniffs, Robot Spiders, and the Contraband Exception to the Fourth Amendment*, 7 CHARLESTON L. REV. 111, 113 (2012) (discussing the issue of whether the sniff by the drug dog constituted a search).

122. *See Jardines*, 73 So. 3d at 50–54; *see also* Owsley, *supra* note 113, at 368–70.

123. *See Jardines*, 569 U.S. at 5.

124. *Id.* (quoting *United States v. Knotts*, 460 U.S. 276, 286 (1983)) (Brennan, J., concurring in judgment).

125. *See Jardines*, 569 U.S. at 6–7; *see also* Owsley, *supra* note 112, at 371 ("[T]he protection of the home from unreasonable searches has long included the house's curtilage.").

126. *Jardines*, 569 U.S. at 8.

127. *Id.* at 8 (quoting *Kentucky v. King*, 563 U.S. 452, 469 (2011)); *see also* Owsley, *supra* note 113, at 372 ("This implicit license applies to law enforcement officers in the same manner as it does to private citizens.").

requires a broader license than the one commonly given to the general public. The Court determined that without such a license, the officers' search violated the Fourth Amendment. Approaching the front door with a trained drug dog was clearly beyond the scope of the ordinary license.¹²⁸

The majority opinion does not address reasonable expectation of privacy. Justice Scalia noted that the Court did not need to decide whether there was a violation of Jardines' reasonable expectation of privacy based on *Katz*.¹²⁹ Instead, as in *Jones*, the decision's reasoning was based on a trespass theory of the Fourth Amendment.

Justice Alito, joined by Chief Justice Roberts as well as Justices Breyer and Kennedy, issued a dissenting opinion.¹³⁰ He argued that the majority interpreted too narrowly the public license to approach a person's front door.¹³¹ This license should extend even to police officers gathering evidence for a criminal case against the resident.¹³² The common law of trespass did not limit the public license to a particular category of visitors approaching the door for a specific purpose.¹³³

III. LAW ENFORCEMENT CAN USE CELL-SITE SIMULATORS TO GATHER DATA FROM CELL PHONES

A. A Cell Phone Operates by Sending and Receiving Radio Waves to a Cell Tower, and a Cell Site Simulator Mimics a Cell Tower to Gather Data

In order to understand how a cell-site simulator works, one first needs to understand how a cell phone works. A cell phone has a dual function, operating simultaneously as a radio transmitter and a radio receiver.¹³⁴ The phone converts the

128. See *Jardines*, 569 U.S. at 9; see also Owsley, *supra* note 112, at 372.

129. In a concurring opinion by Justice Kagan, joined by Justices Ginsburg and Sotomayor, she argued that the case also concerned privacy issues along with the property and trespass issues raised by the majority opinion. See *Jardines*, 569 U.S. at 12 (Kagan, J., concurring). Homeowners have a heightened expectation of privacy in their homes and the curtilage. Here, the police violated Jardines' reasonable expectation of privacy as established in *Kyllo* (and *Katz*). See *Jardines*, 569 U.S. at 12, 14 (Kagan, J., concurring); see also Owsley, *supra* note 112, at 373 (Justice Kagan "explained that analysis of the case according to a right to privacy theory would have led to the conclusion that *Kyllo* resolved the issue."). Because the police officers used a drug-sniffing dog, a device not in public use, to obtain intimate information about the home, the search violated the Fourth Amendment. See *Jardines*, 569 U.S. at 14–15 (Kagan, J., concurring).

130. See *Jardines*, 569 U.S. at 16 (Alito, J., dissenting).

131. See *id.*

132. See *id.* at 19–21.

133. See *id.* at 21.

134. See Stephanie K. Pell & Christopher Soghoian, *A Lot More than a Pen Register, and Less than a Wiretap: What the StingRay Teaches Us about How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities*, 16 YALE J.L. & TECH. 134, 144–45 (2013); see also *In re United States for Historical Cell Site Data*, 747 F. Supp. 2d 827, 831 (S.D. Tex. 2010) (" . . . [C]ellular telephones use radio waves to communicate between the user's handset and the telephone network."); *In re Pen Register and Trap and Trace Device with Cell Site Location Authority*, 396 F. Supp. 2d 747, 750 (S.D. Tex. 2005) ("A cell phone is a sophisticated two-way radio with a low-power transmitter that operates in a network of cell sites.").

user's voice into electrical signals, transmits those signals via radio waves, and similarly converts incoming electrical signals into the other speaker's voice.¹³⁵

Cell phones function within "cells" that provide service covering about a ten-square-mile area.¹³⁶ The cell-site or cellular base station consists of a large antenna and electronic equipment that receives and transmits radio signals from cell phones.¹³⁷ As the cell phone user moves, the service shifts to adjacent cells with their base stations.¹³⁸ Thus, a caller can drive down the highway and maintain the connection mile after mile.

Cell phone calls are transmitted by radio waves from the cell phone to the nearest cell towers.¹³⁹ Then the calls are relayed along a series of cell towers until the call reaches the other cell phone.¹⁴⁰ When cell phones are turned on but not in use, they register constantly with the nearest network cell towers in order to be available should a call come into the cell phone or be made from the cell phone.¹⁴¹

A cell-site simulator functions by mimicking a cell phone tower, enabling it to capture information from as many as 60,000 cell phones at the same time.¹⁴² When the nearby cell phones seek to register with a cell tower, the cell-site simulator creates the impression that it is a cell tower, capturing the cell phones' data, including

135. See *In re Pen Register*, 396 F. Supp. 2d at 751 (S.D. Tex. 2005).

136. See Henry H. Perritt, Jr., *The Internet Adopts Two-Way Radio*, 10 HASTINGS SCI. & TECH. L.J. 147, 157 (2019); see, e.g., *Nextel of N.Y., Inc. v. Assessor for Spring Valley*, 771 N.Y.S. 2d 853, 860 (N.Y. Sup. Ct. 2004).

137. See Perritt, *supra* note 136, at 157–58; Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now?: Toward Reasonable Standards for Law Enforcement Access to Location Data that Congress Could Enact*, 27 BERKELEY TECH. L.J. 117, 126, 136–37 (2012) (citing U.S. DEP'T OF JUSTICE (DOJ) SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 160 (3d ed. 2009), available at <http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf>).

138. See *In re United States for an Ord. for Disclosure of Telecomms. Recs.*, 405 F. Supp. 2d 435, 437 (S.D. N.Y. 2005) ("As a cell phone user moves from place to place, the cell phone automatically switches to the tower that provides the best reception."); see also Pell & Soghoian, *supra* note 137, at 127 ("[M]obile telephones (as their name suggests) are portable, and so when a phone moves away from the cell site with which it started a call and nearer to a different cell site, the call is 'handed over' from one cell site to another without interruption.").

139. See *In re United States for an Ord. for Disclosure of Telecomms. Recs.*, 405 F. Supp. 2d at 436–37.

140. See, e.g., Pell & Soghoian, *supra* note 137, at 144.

141. See *In re United States for an Ord. Directing a Provider of Elec. Commc'n Serv. to Disclose Recs. to the Gov't*, 534 F. Supp. 2d 585, 589–90 (W.D. Pa. 2008) (citation omitted), *rev'd on other grounds* 620 F.3d 304, 313 (3d Cir. 2010); see also *State v. Copes*, 165 A.3d 418, 423 (Md. 2017) (cell-site simulators function because "a cell phone—when turned on—constantly seeks out nearby cell towers, even if the user is not making a call"); Kim Zetter, *How Cops Can Secretly Track Your Phone*, THE INTERCEPT (July 31, 2020, 7:00 a.m.), <https://theintercept.com/2020/07/31/protests-surveillance-stingrays-dirtboxes-phone-tracking/>.

142. See *United States v. Artis*, 315 F. Supp. 3d 1142, 1144 (N.D. Cal. 2018) (A cell-site simulator "'tricks' nearby cell phones into thinking that it's a cell tower, thereby causing nearby cell phones to send signals to the device, which allows the operator of the device to locate the phone being sought."); see, e.g., *State v. Sylvestre*, 254 So.3d 986, 989–90 (Fla. Ct. App. 2018) (quoting *Artis*); see also *United States v. Lambis*, 197 F. Supp. 3d 606, 609 (S.D.N.Y. 2016) ("A cell-site simulator—sometimes referred to as a 'StingRay,' 'Hailstorm,' or 'TriggerFish'—is a device that locates cell phones by mimicking the service provider's cell tower (or 'cell-site') and forcing cell phones to transmit 'pings' to the simulator."); Elyssa Cherney, *Chicago Lawyer Files Federal Lawsuit over Police Cellphone Tracking System*, CHICAGO TRIBUNE (Jan. 13, 2017).

the cell phone number.¹⁴³ In other words, the cell-site simulator can only target and obtain information from cell phones that are turned on.¹⁴⁴ When a nearby cell phone is on, a cell-site simulator forces the cell phone to emit information.¹⁴⁵

The cell phone operates on a network, typically 4G, which employs strong encryption. The cell-site simulator jams the 4G network and the 3G network, forcing the cell phone to operate on a 2G network. At that level, security is greatly diminished, and the cell-site simulator can cause “the phone to use either no encryption or use a weak encryption that can be cracked.”¹⁴⁶ Thus, the only available network for the cell phone to register is the one temporarily controlled by the cell-site simulator.¹⁴⁷

Theoretically, the capture of the data is so brief that the simulator should not adversely impact the cell phone’s service even if it is currently in use for a call.¹⁴⁸ However, “once the cell-site simulator ‘grabs’ the target phone, the target phone is prevented from communicating ‘with an actual . . . tower.’”¹⁴⁹ For example, in *Jones*, the court explained that “because the cell-site simulator is not a true cell tower connected with the cellular network, any cellphone connected to the cell-site simulator will not be able to communicate with the network: ‘[Y]our call doesn’t go through[,] period. Nothing happens.’”¹⁵⁰ The Department of Justice has represented in federal court that the use of a cell-site simulator can disrupt the use of a cell phone: “Assistant United States Attorney Osmar J. Benvenuto told a federal court in New Jersey, ‘Because of the way the Mobile Equipment sometimes operates, its use has the potential to intermittently disrupt cellular service to a small fraction of Sprint’s wireless customers within its immediate vicinity.’”¹⁵¹

Moreover, when law enforcement activates such a device, it will “send signals, often indiscriminately, through the walls of homes, vehicles, purses, and pockets in order to probe and identify the phones located inside.”¹⁵² Once the data is

143. See *State v. Tate*, 849 N.W. 3d 798, 802 n.8 (Wis. 2014) (citation omitted); *State v. Andrews*, 134 A.3d 324, 341 (Md. App. 2016); Pell & Soghoian, *supra* note 134, at 142, 145–46 (2014).

144. See *United States v. Tutis*, 216 F. Supp. 3d 467, 481 (D.N.J. 2016) (A cell-site simulator “would invite its electronic signal exchange only from active cell phones; if in the home one did not wish to communicate identifying data, one need only turn the cell phone off.”).

145. See *Andrews*, 134 A.3d at 333; *Lambis*, 197 F. Supp. 3d at 615 (citing *Andrews*, 134 A.3d at 324, *Tate* 849 N.W. 3d at 798).

146. See Zetter, *supra* note 141; see also *Jones v. United States*, 168 A.3d 703, 713, n.21 (D.C. 2017) (“[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.”).

147. See Zetter, *supra* note 141.

148. U.S. DEP’T OF JUST., POLICY GUIDANCE: USE OF CELL-SITE SIMULATOR TECHNOLOGY 5 (Sept. 3, 2015), <https://www.justice.gov/opa/file/767321/download>.

149. *Jones*, 168 A.3d at 709.

150. *Id.* at 710 (citing testimony by an expert witness for the defense on cell phone technology).

151. Complaint for Relief Against Unauthorized Radio Operation and Willful Interference with Cellular Communications at 14; *In re Balt. City Police Dep’t*, (FCC Rcd. Aug. 16, 2016).

152. 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 (2014).

captured, the cell phone is released by the device, returning to the proper cell phone network. Typically, a laptop computer is connected to the cell-site simulator and used to download the cell phone data on it.¹⁵³

B. There Are an Array of Different Cell-site Simulators with Different Features

Law enforcement officers use cell-site simulators to locate cell phones in the course of their criminal investigative work. The Harris Corporation makes many of these devices, including the StingRay, Amberjack, Harpoon, and Kingfish.¹⁵⁴ It has sold many such devices to state and local law enforcement through grants from the Department of Homeland Security based on a sole-source contract with that agency.¹⁵⁵

Harris Corporation conceals information, including in some sales brochures, about the electronic surveillance technologies that it sells to government agencies based on national security concerns.¹⁵⁶ Moreover, the federal government has non-disclosure agreements with state and local law enforcement agencies that purchase cell-site simulators.¹⁵⁷ For example, the Baltimore City Police Department signed a non-disclosure agreement with the FBI when it purchased a Hailstorm from the Harris Corporation.¹⁵⁸ Specifically, the agreement bars the police department from using or providing in any criminal or civil action “any information concerning the Harris Corporation wireless collection equipment/technology, its associated software, operating manuals, and any related documentation (including its technical/engineering description(s) and capabilities).”¹⁵⁹ Moreover, if either the police department or the State’s Attorney for Baltimore City discover that a circumstance exists that may result in disclosure of such information, they must immediately contact the FBI so that it may seek to intervene.¹⁶⁰ Indeed, “the government has gone so far as to dismiss cases and withdraw evidence rather than reveal that the technology was used.”¹⁶¹

153. Brian L. Owsley, *TriggerFish, StingRays, and Fourth Amendment Fishing Expeditions*, 66 HASTINGS L.J. 183, 213 (2014); U.S. DEP’T OF JUSTICE, ELECTRONIC SURVEILLANCE 44, 171-74 (rev. 2005).

154. *See id.*; Ryan Gallagher, *Meet the machines that steal your phones data*, ARS TECHNICA (Sept. 25, 2013, 1:00 p.m.), <https://arstechnica.com/tech-policy/2013/09/meet-the-machines-that-steal-your-phones-data/>.

155. *See* Owsley, *supra* 153; Gallagher, *supra* note 154.

156. *See* Gallagher, *supra* note 154.

157. *See* Robert Patrick, St. Louis police: We track cellphones, but won’t tell you how, ST. LOUIS POST-DISPATCH, (May 25, 2015), <https://perma.cc/7UAN-ZD7L>; *see also In re United States for an Ord. Relating to Telephones Used by Suppressed*, No. 15 M 0021, 2015 WL 6871289, at *1 (N.D. Ill. Nov. 9, 2015) (finding that Harris Corporation, the major manufacturer of cell-site simulators, has non-disclosure agreements with state and local law enforcement agencies).

158. *See* *Andrews v. Baltimore City Police Dep’t*, Civil No. CCB-16-2010, 2018 WL 3649602, at *2 (D. Md. Aug. 1, 2018).

159. *Id.* at *3.

160. *See id.*

161. *United States v. Patrick*, 842 F.3d 540, 545 (7th Cir. 2016); *see also* Jessica Lussenhop, St. Louis Police Have Used StingRay Technology For Years—They Just Won’t Talk About It, *Riverfront Times* (May 20, 2015,

Cell-site simulators like the StingRay can access communications content such as audio and text messages from cell phones.¹⁶² They are portable, and police officers can install them within police vehicles.¹⁶³

The policy guidance from the Department of Justice regarding the use of cell-site simulators mandates that they must be configured as pen registers, and prohibits the collection of audio communications.¹⁶⁴ The wiretap statute bars the government from obtaining such communications without a warrant.¹⁶⁵ In addition to such communications, this ban includes data on the cell phone such as “emails, texts, contact lists, images or any other data from the phone.”¹⁶⁶ Of course, after *Riley v. California*,¹⁶⁷ obtaining this type of data from a cell phone requires a search warrant.

In a Harris Corporation promotional brochure, it describes a KingFish as “a multiprotocol, cellular communications system . . . [it] is a man-portable, single receiver, single transmitter platform capable of supporting multiple, cellular communications technologies.”¹⁶⁸ In other words, it is “a smaller hand-held device that operates like a stingray and can be used by a law enforcement agent while walking around outside a vehicle.”¹⁶⁹ Interestingly, Harris Corporation has a distribution warning at the bottom of its KingFish brochure, noting that it “may be provided only to persons eligible under 28 U.S.C. § 2512 (Government law enforcement agencies or communications service providers).”¹⁷⁰

In another promotional brochure, the Harris Corporation describes a Harpoon as “software-controlled, high-power filtered amplifier that maximizes the multichannel transmit capability of the StingRay II (mark omitted) and significantly improves the performance of the single-channel StingRay (mark omitted) and KingFish (mark omitted) systems by providing high-gain, wide dynamic range . . .”¹⁷¹ In other words, a Harpoon boosts the signals of StingRay and KingFish

8:00 a.m.), <https://perma.cc/P6HK-M6F3> (“In a handful of incidents around the country, prosecutors have dropped cases, offered plea deals or withdrawn evidence rather than disclose information about StingRay.”).

162. See Pell & Soghoian, *supra* note 152, at 146.

163. See Lussenhop, *supra* note 161.

164. “Moreover, cell-site simulators used by the Department must be configured as pen registers, and may not be used to collect the contents of any communication, in accordance with 18 U.S.C. § 3127(3).” See U.S. DEP’T OF JUST., POLICY GUIDANCE: USE OF CELL-SITE SIMULATOR TECHNOLOGY 2 (Sept. 3, 2015), <https://www.justice.gov/opa/file/767321/download>.

165. See 18 U.S.C. § 2518.

166. U.S. DEP’T OF JUST., POLICY GUIDANCE: USE OF CELL-SITE SIMULATOR 3 (Sept. 3, 2015), <https://www.justice.gov/opa/file/767321/download>.

167. 573 U.S. 373, 381–403 (2014) (finding that the warrantless search exception following an arrest exists for two reasons—preserving evidence and protecting officer safety—but neither basis exists regarding cell phone searches incident to arrest and thus law enforcement needs a search warrant).

168. HARRIS CORPORATION, KINGFISH, <https://perma.cc/6A3S-A78Z> (last visited September 4, 2021).

169. See Zetter, *supra* note 141.

170. HARRIS CORPORATION, KingFish, <https://perma.cc/6A3S-A78Z> (last visited September 4, 2021).

171. HARRIS CORPORATION, Harpoon, <https://cdn.arstechnica.net/wp-content/uploads/2013/09/harpoon.pdf> (last visited September 1, 2021).

devices.¹⁷² Again, the brochure has the same distribution warning as the KingFish brochure.¹⁷³

In a Harris Corporation brochure, the company describes an AmberJack as “a phased array direction-finding . . . antenna capable of providing lines to mobile phone users and base stations” when used with various Harris cell-site simulator devices.¹⁷⁴ This antenna merges “Harris’ expertise in phased array antenna technology and location based services to offer a state-of-the-art direction-finding system.”¹⁷⁵ In other words, this antenna helps home in on the location of a particular cell phone.

Dirtboxes, which are cell-site simulators that are used in small aircraft to surveil a larger area, are manufactured by Digital Receiver Technology, which is a subsidiary of Boeing.¹⁷⁶ The United States Marshal Service and the FBI mount these devices on a small plane such as a Cessna.¹⁷⁷ “An air-borne dirtbox has the ability to collect data on many more phones than a ground-based stingray; it can also move more easily and quickly over wide areas.”¹⁷⁸

GammaGroup is an English-German company manufacturing a range of cell-site simulators, including its Model 4019 HP with “active interception solutions [that] provide[] a tactical tool for Law Enforcement, Government and Military Agencies.”¹⁷⁹ A sales brochure also notes that it has Model ANT 8000, which is a vehicular system; Model 4062, which is a cell-site simulator worn on the body under clothing; Model 4061, which is located in a portable briefcase, as well as other tracking and geo-locating devices.¹⁸⁰

C. Law Enforcement Officers Can Use Cell-site Simulators in Three Different Manners

Cell-site simulators can be used in a few different ways. In the first scenario, if the investigating law enforcement officers already know the suspect’s cell phone

172. See Zetter, *supra* note 141.

173. See HARRIS CORPORATION, *Harpoon*, <https://cdn.arstechnica.net/wp-content/uploads/2013/09/harpoon.pdf> (last visited September 1, 2021); HARRIS CORPORATION, *KingFish*, <https://perma.cc/6A3S-A78Z> (last visited September 4, 2021).

174. HARRIS CORPORATION, *Amberjack*, https://www.nyclu.org/sites/default/files/AmberJack_ProductDescription.pdf (last visited September 1, 2021).

175. *Id.*

176. See generally Brian L. Owsley, *Spies in the Skies: Dirtboxes and Airplane Electronic Surveillance*, 113 MICH. L. REV. FIRST IMPRESSIONS 75–76 (2015) (explaining the purpose and usage of dirtboxes).

177. See Zetter, *supra* note 141.

178. *Id.*

179. GAMMAGROUP, *3G-GSM Tactical Interception & Target Location*, at 15, <https://info.publicintelligence.net/Gamma-GSM.pdf> (last visited September 1, 2021); see also GAMMAGROUP, *Products and Services*, <https://www.gammagroup.com/ProductsServices.aspx?m=p> (last visited September 1, 2021) (providing overview of all of GammaGroup’s products and services).

180. GAMMAGROUP, *Products and Services*, <https://www.gammagroup.com/ProductsServices.aspx?m=p> (last visited September 1, 2021) (providing overview of all of GammaGroup’s products and services).

number, then they can target that known number in a search for the suspect.¹⁸¹ As an initial step, the officers obtain the targeted cell phone's subscriber information as well as the real-time location information from the cell phone's telecommunications provider.¹⁸² This approach, consistent with a search warrant, would generally be a constitutionally permissible use of a cell-site simulator because the search is done with particularity and specificity by targeting a known cell phone (and number).¹⁸³ For example, a former state court judge in St. Louis, Missouri, acknowledged that he would sign a warrant authorizing the use of a cell-site simulator when the application included the cell phone's serial number and the cell phone provider.¹⁸⁴

In the second scenario, law enforcement officers may have a suspect for a criminal investigation, but they do not have a cell phone number associated with that suspect. During the course of surveillance of this suspect, they will follow that person to several different locations and use the cell-site simulator.¹⁸⁵ For example, they will use the device at the suspect's home in the morning. If the person then goes to a restaurant for lunch, the device will be used there. In the evening, the person may go out to socialize or meet with friends; law enforcement will use the cell-site simulator at that location. Of course, as law enforcement is targeting the suspect, it is also gathering private data regarding all of cell phones in the vicinity. As

181. See *United States v. Lambis*, 197 F. Supp. 3d 606, 609 (S.D.N.Y. 2016) (finding that a technician used a cell-site simulator to locate defendant's precise location); *In re United States for an Ord. Relating to Telephones Used by Suppressed*, No. 15 M 0021, 2015 WL 6871289, at *2 (N.D. Ill. Nov. 9, 2015) ("Armed with a cell-site simulator, a law enforcement officer can obtain a target's cell phone's ESN or IMSI (among many other things) by taking the device near the physical location of the target's cell phone and then activating the device."); *Jones v. United States*, 168 A.3d 703, 709 ("The officers operating the cell-site simulator drive around and 'as soon as the [the simulator] comes across [the target phone's signal] it grabs it and it holds on to it. Once the cell-site simulator 'grabs' the target phone, the simulator begins reporting 'general location information and signal strength' that can be used to locate the target phone's exact location.") (internal quotations omitted).

182. *Jones*, 168 A.3d at 712.

183. But see *United States v. Powell*, No. 2:18-cv-13107, 2020 WL 3868500, at *4 (E.D. Mich. July 9, 2020), *appeal filed*, No. 20-1894 (6th Cir. Sept. 17, 2020) (finding that where a cell-site simulator is only used to obtain a suspect's cell phone numbers, there is no Fourth Amendment violation because one does not have a reasonable expectation of privacy in one's phone number); see also *United States v. Patrick*, 842 F.3d 540, 543 (7th Cir. 2016) ("One potential question posed by use of a cell-site simulator would be whether it is a 'search' at all, or is covered by *Smith v. Maryland*, 442 U.S. 735 (1979) and *United States v. Knotts*, 460 U.S. 276 (1983).").

184. See Lussenhop, *supra* note 161.

185. See, e.g., *United States v. Tutis*, 216 F. Supp. 3d 467, 472 (D.N.J. 2016) (Law enforcement obtained the warrant for the cell-site simulator to "canvass all cells phones within close proximity to Tutis at one location and then do so again at other known Tutis locations, yielding list of identifying data for each vicinity's cell phones. Then by 'process of elimination' the detectives could focus upon the common cell phone number(s) that showed up at each Tutis location, which logically would be highly probably possessed by Tutis, and thus lead to the identification of a new Tutis cell phone."); *Powell*, 2020 WL 3868500, at *4 ("The cell-site simulator was therefore used only to obtain the numbers of the various phones that Defendant used and not to verify his location."); *United States v. Johnson*, No. 4:18 CR 565, 2020 WL 3989590, at *2 (E.D. Mo. July 15, 2020) ("The purpose of [using a cell-site simulator] was to identify a cell phone or phones used by Johnson as part of his drug distribution activities. Authorities used the cell site simulator in 'canvass' mode in different location in Johnson's vicinity.").

Professor Tim Nolan, a former Boston Police Department lieutenant, explained about the confusion for law enforcement regarding this private data:

Say I'm looking at a drug dealer on a corner, and we sweep up data on hundreds of people who happen to be in the vicinity. And then, at some later point, we realize there was some unrelated incident there, too . . . Do I now have the right to access that data, even if we had no probable cause about any particular individuals?¹⁸⁶

Ultimately, law enforcement will use the cell-site simulator in enough locations where they have surveilled the suspect so that they will have captured numerous cell phone numbers in each location. They will analyze the data from each location and look for common cell numbers at all or most of the locations. Those numbers will then become the next step in the investigation of the suspect and the criminal enterprise. Of course, at each location, not only are the police gathering the cell phone numbers of the persons who are the target of the investigation or involved in the criminal conduct, but they are also getting access to the data of a large number of innocent people.¹⁸⁷

In the last scenario, there is a circumstance where law enforcement uses a cell-site simulator without any specific target.¹⁸⁸ For example, there may be a large gathering of people at a protest or rally, and the police want to determine who is present. Indeed, if they do it over several days of a protest, they might determine who is always present and possibly who serves in leadership positions of the protest groups.

IV. THE USE OF CELL-SITE SIMULATORS CONSTITUTES A SEARCH

In 2015, the United States Department of Justice issued new policy guidance altering its internal policies indicating that, generally, the government would seek a search warrant before using a cell-site simulator.¹⁸⁹ However, as one court noted, federal officers would do this *ordinarily*, but not always, and the Department of

186. George Joseph, *Racial Disparities in Police 'Stingray' Surveillance, Mapped*, BLOOMBERG NEWS, (Oct. 16, 2016, 7:00 AM), <https://www.bloomberg.com/news/articles/2016-10-18/u-s-police-cellphone-surveillance-by-stingray-mapped> (quoting Tim Nolan, an associate professor of criminology at Merrimack College and former Boston Police Department Lieutenant).

187. See Zetter, *supra* note 141; Kim Zetter, *The Feds Are Now Using 'Stingrays' in Planes to Spy on Our Phone Calls*, WIRED (Nov. 14, 2014, 2:14 PM), <http://www.wired.com/2014/11/feds-motherfng-stingrays-motherfng-planes/>.

188. See Zetter, *supra* note 141 ("Law enforcement can also use a stingray in a less targeted way to sweep up information about all nearby phones.").

189. See *United States v. Lambis*, 197 F. Supp. 3d 606, 611 (S.D.N.Y. 2016) (citing U.S. Dep't of Just., *Deputy Assistant General Richard Downing Testifies Before House Oversight and Government Reform Committee At Hearing on Geolocation Technology and Privacy*, JUSTICE NEWS (Mar. 16, 2016), <https://www.justice.gov/opa/speech/deputy-assistant-attorney-general-richard-downing-testifies-house-oversight-and>; U.S. Dep't of Just., *Justice Department Announces Enhance Policy for Use of Cell-Site Simulators*, JUSTICE NEWS (Sept. 3, 2015), <https://www.justice.gov/opa/pr/justice-department-announces-enhanced-policy-use-cell-site-simulators>).

Justice did “not concede[] that this [warrant] is constitutionally required.”¹⁹⁰ Federal law enforcement officials do not indicate that the use of a cell-site simulator is controlled by the Fourth Amendment. Moreover, this policy guidance does not apply to state and local law enforcement officers.

In order for a search to have occurred, a governmental official or agent of the government must intrude into an individual’s home, person, papers, or effects in a manner that breaches some privacy interest of that individual. There are two components. First, there must be some kind of intentional state action.¹⁹¹ Second, there must be an intrusion within the sphere that the individual reasonably holds as private.¹⁹²

In some respects, the notion of what constitutes a search appears to be a straightforward proposition. Since the Bill of Rights, Justice Scalia explained that the word “search” has had a similar meaning: “[t]o look over or through for the purpose of finding something; to explore; to examine by inspection; as, to *search* the house for a book.”¹⁹³ However, Justice Scalia further noted that the “question whether or not a Fourth Amendment ‘search’ has occurred is not so simple under our precedent.”¹⁹⁴ That lack of simplicity is further exacerbated when technology is involved.

A. The Supreme Court Has Not Explicitly Addressed Cell-Site Simulators, But Its Decisions Provide Some Guidance

Historically, the federal government sought court authorization for cell-site simulators pursuant to a pen register.¹⁹⁵ The Supreme Court has explained that a pen register is “a device that records telephone numbers dialed from a *particular phone*.”¹⁹⁶ The pen register statute requires a very low standard. Law enforcement officials need only provide “a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency” to obtain a pen register.¹⁹⁷

Historically, the Department of Justice provided guidance to obtain orders authorizing cell-site simulators based on this low standard.¹⁹⁸ In September 2015,

190. *United States v. Patrick*, 842 F.3d 540, 545 (7th Cir. 2016).

191. *See United States v. Jacobsen*, 466 U.S. 109, 113 (1984); *United States v. Fortney*, 772 F. App’x 269, 272–73 (6th Cir. 2019).

192. *See Jacobsen*, 466 U.S. at 113.

193. *Kyllo v. United States* 533 U.S. 27, 32 n.1 (2001) (quoting N. WEBSTER, AN AMERICAN DICTIONARY OF THE ENGLISH LANGUAGE 66 (1828) (reprint 6th ed. 1989)).

194. *Id.* at 31.

195. *See In re United States for an Ord. Authorizing the Installation and Use of a Pen Register and Trap and Trace Device*, 890 F. Supp. 2d 747, 749 (S.D. Tex. 2012).

196. *United States v. Giordano*, 416 U.S. 505, 511 n.2 (1974) (emphasis added); *accord United States v. Lambis*, 197 F. Supp. 3d 606, 608 (S.D.N.Y. 2016); *see also 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.”).

197. 18 U.S.C. § 3122(a)(2).

198. U.S. DEP’T OF JUST., ELECTRONIC SURVEILLANCE 44, 171–74 (rev. 2005).

the Department of Justice announced that it would establish probable cause when seeking court authorization for a cell-site simulator.¹⁹⁹ This policy guidance, along with the Supreme Court decisions below, bolster the notion that the cell-site simulators violate general warrant principles even though the Supreme Court has not explicitly addressed the issue.

1. The Use of Thermal Imaging Devices Violates the Fourth Amendment

In *Kyllo v. United States*,²⁰⁰ the Supreme Court addressed a new technology, a thermal imaging device: “Thermal imagers detect infrared radiation, which virtually all objects emit but which is not visible to the naked eye.”²⁰¹

Based on suspicion that Kyllo was growing marijuana in his home, federal agents used a thermal-imaging device to detect heat emanating from his triplex home at 3:20 a.m.²⁰² A federal agent conducted this scan with the device in just a few minutes while sitting in a vehicle parked across the street from Kyllo’s house.²⁰³ The scan revealed that part of his house was significantly hotter than the rest of his house and much warmer than the other homes in the triplex.²⁰⁴ The agent determined that this amount of heat coming from his home was consistent with the high-intensity lamps that could be used for growing marijuana inside. Based on the informants’ statements, Kyllo’s electric bills, and the results from the thermal imaging, police obtained a search warrant for the home from a federal magistrate judge.²⁰⁵ During the search, police discovered over one hundred marijuana plants.²⁰⁶

The Court addressed whether the use of a thermal-imaging device to detect the heat radiating from Kyllo’s home was a search pursuant to the Fourth Amendment.²⁰⁷ The Court held that when police obtain information about the inside of a home without physical intrusion, using a device not normally used by the public, the police action constitutes a Fourth Amendment search and is presumptively unreasonable without a warrant.²⁰⁸

199. U.S. DEP’T OF JUST., POLICY GUIDANCE: USE OF CELL-SITE SIMULATOR TECHNOLOGY 3 (Sept. 3, 2015), <https://www.justice.gov/opa/file/767321/download>.

200. 533 U.S. 27 (2001).

201. *Id.* at 29.

202. *See id.*

203. *See id.* at 30.

204. *See id.*

205. *See id.*

206. *See id.*

207. *See id.* at 29.

208. *See id.* at 40.

2. Law Enforcement Must Obtain a Search Warrant in Order to Obtain Cell Site Location Information

In *Carpenter v. United States*, the Supreme Court addressed whether the Government's obtaining of an individual's cell site location information from his telephone provider constituted a search.²⁰⁹ Timothy Carpenter challenged the use of this cell phone data insofar as the Government did not obtain a search warrant.²¹⁰ Specifically, he argued that the historical cell site location data required a warrant based on probable cause instead of an order pursuant to the Stored Communications Act,²¹¹ which is what the Government had obtained.²¹²

Police arrested four men for armed robberies of Radio Shack and T-Mobile stores in Detroit.²¹³ One man confessed to a role in nine separate robberies in Michigan and Ohio with a group of at least fifteen men who communicated by cell phones.²¹⁴ Moreover, he provided the FBI some of his accomplices' cell phone numbers as well as his records to reveal who he called around the time of the robberies.²¹⁵ With this information, the Assistant United States Attorneys obtained court orders pursuant to the Stored Communications Act for the cell phone data of Carpenter and several other suspects.²¹⁶ Specifically, the cell phone providers' records provided data regarding Carpenter for 127 days and regarding Timothy Sanders for eighty-eight days.²¹⁷

At trial, seven accomplices testified that Carpenter organized the robberies and provided the weapons.²¹⁸ Moreover, Carpenter and Sanders served as lookouts waiting nearby in a stolen car.²¹⁹ Carpenter provided a signal from this vehicle that indicated to the others to commence the armed robbery.²²⁰

In addition to the seven accomplices, the Government also provided expert testimony by FBI agent Michael Hess regarding cell site data of nearby cell towers for cell phones used by Carpenter and Sanders.²²¹ Specifically, "Hess explained that each time a cell phone taps into the wireless network, the carrier logs a time-stamped record of the cell site and particular sector that were used."²²² Based on

209. *Carpenter v. United States*, 138 S. Ct. 2206, 2211 (2018).

210. *Id.* at 2212.

211. *Id.*; see also 18 U.S.C. § 2703(d).

212. See *Carpenter*, 138 S. Ct. at 2212.

213. See *id.*

214. See *id.*

215. See *id.*

216. See *id.*

217. See *id.*; *United States v. Carpenter*, 819 F.3d 880, 886 (6th Cir. 2016), *rev'd*, 585 U.S. ___, 138 S. Ct. 2206 (2018).

218. See *Carpenter*, 138 S. Ct. at 2212; *Carpenter*, 819 F.3d at 884–85.

219. See *Carpenter*, 819 F.3d at 884–85.

220. See *id.* at 885.

221. See *Carpenter*, 138 S. Ct. at 2212–13; *Carpenter*, 819 F.3d at 885.

222. *Carpenter*, 138 S. Ct. at 2212; see also *Carpenter*, 819 F.3d at 885 (summarizing the FBI agent Hess' testimony regarding how cell phones operate through a series of cell towers and radio connections).

this data, “Hess produced maps that placed Carpenter’s phone near four of the charged robberies.”²²³ The jury convicted Carpenter on several counts, and he received a 100-year sentence.²²⁴

The Supreme Court granted the petition for a writ of certiorari to address whether the Government’s obtaining of the historical cell site location information without a search warrant violated the Fourth Amendment.²²⁵ The Court held that obtaining the cell site location records without a warrant violated the Fourth Amendment ban against unreasonable searches and seizures.²²⁶

Writing for the majority, Chief Justice Roberts noted that the Fourth Amendment protects both property interests as well as reasonable expectations of privacy.²²⁷ Even though people like Carpenter engage in conduct within the public sphere, they still maintain some Fourth Amendment protection within that sphere.²²⁸ The Court declined to extend the third-party doctrine²²⁹ to Carpenter’s cell site location information because the intrusive nature of such data would provide law enforcement officers with a significant invasion of the cell phone user’s privacy.²³⁰ Indeed, the privacy rights at issue here with historical cell site location records are arguably greater than those presented regarding GPS tracking in *Jones*.²³¹ Thus, law enforcement needs to obtain a search warrant to review cell site location information absent exigent circumstances.²³² Further, review of cell site location information constitutes a search.²³³

223. *Carpenter*, 138 S. Ct. at 2213; *accord Carpenter*, 819 F.3d at 885 (“With the cell-site data provided by Carpenter’s and Sanders’s wireless carriers, Hess created maps showing that Carpenter’s and Sanders’ phones were within a half-mile to two miles of the location of each of the robberies around the time the robberies happened.”).

224. *See Carpenter*, 138 S. Ct. at 2213.

225. *See id.* at 2212.

226. *See id.* at 2221.

227. *See id.* at 2213.

228. *See id.* at 2217; *see generally* Antony Barone Kolenc, “23 and Plea”: *Limiting Police Use of Genealogy Sites after Carpenter v. United States*, 122 W. VA. L. REV. 53, 54–55, 96 (2019) (arguing that, after *Carpenter*, there may be an enforceable privacy right in information shared with genealogy websites, such as “23 and Me”).

229. The Supreme Court developed the third-party doctrine to reduce Fourth Amendment protections when an individual voluntarily shares access to that person’s personal information by establishing that there is no longer a reasonable expectation of privacy in that information. *See generally* Brian L. Owsley, *Cell Phone Tracking in the Era of United States v. Jones and Riley v. California*, 48 TEX. TECH. L. REV. 207, 217–19 (2015) (discussing *Smith v. Maryland*, 442 U.S. 735 (1979) and *United States v. Miller*, 425 U.S. 435 (1976)).

230. *See Carpenter*, 138 S. Ct. at 2217; *see also id.* at 2209–10 (finding that government access to cell site location information invaded “the whole of [Carpenter’s] physical movements” and would provide a detailed chronicle of their physical presence).

231. *See id.* at 2210 (“[I]n fact, historical cell-site records present even greater privacy concerns than the GPS monitoring considered in *Jones*.”).

232. *See id.* at 2221–22.

233. *See id.* at 2222 (“If the third-party doctrine does not apply to the ‘modern-day equivalents of an individual’s own “papers” or “effects,” then the clear implication is that the documents should receive full Fourth Amendment protection. We simply think that such protection should extend as well to a detailed log of a person’s movements over several years.”).

B. Some Courts Have Specifically Concluded a Warrant Is Required When the Police Use Cell-Site Simulators

Only a few courts have addressed issues related to cell-site simulators. In some of those decisions, courts addressed whether the use of this device constituted a search. Several courts concluded that the use of a cell-site simulator is indeed a search for which law enforcement must obtain a search warrant.

A federal district court in New York has determined that a search warrant was necessary before law enforcement could use a cell-site simulator.²³⁴ In *United States v. Lambis*, federal agents were involved in a drug investigation during which they obtained a warrant for both pen register data and cell site location information for a targeted cell phone.²³⁵ Based on that information, the agents were able to pinpoint the target cell phone to within a Manhattan city block.²³⁶ In order to more precisely locate this cell phone, a technician deployed a cell simulator, which led the agents to Raymond Lambis' apartment.²³⁷ After they gained consent to enter, the agents located narcotics and drug paraphernalia, which Lambis filed a motion to suppress.²³⁸

Addressing Lambis' motion to suppress, the trial court first noted that "[a] Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable."²³⁹ Moreover, a warrantless search, like the one in *Lambis*, is generally deemed to be per se unreasonable.²⁴⁰ Additionally, the court explained that one's home is particularly protected pursuant to the Fourth Amendment.²⁴¹

Although the Federal Government argued that there was no search, the *Lambis* court explicitly rejected that position, finding that "[t]he use of a cell-site simulator constitutes a Fourth Amendment search within the contemplation of *Kyllo*. Absent a search warrant, the Government may not turn a citizen's cell phone into a tracking device."²⁴² Thus, the Government needed a search warrant to use this device in conjunction with a cell-site simulator to track Lambis' location.²⁴³

Similarly, a Maryland appellate court ruled that the use of a cell-site simulator was a search that mandated a warrant. In *Andrews v. Baltimore City Police*

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

235. *See Lambis*, 197 F. Supp. 3d at 608; *see also* Carrie Leonetti, *A Hailstorm of Uncertainty: The Constitutional Quandary of Cell-Site Simulators*, 85 U. CINN. L. REV. 665, 690 (2017) (explaining DEA obtained a warrant to "place a pen register and acquire real-time CSLI from Lambis's phone").

236. *See Lambis*, 197 F. Supp. 3d at 609.

237. *See Lambis*, 197 F. Supp. 3d at 609; *see also* Leonetti, *supra* note 235, at 690 (explaining the DEA used a Stingray device to identify Lambis's specific apartment).

238. *See Lambis*, 197 F. Supp. 3d at 609; *see also* Leonetti, *supra* note 235, at 690.

239. *Lambis*, 197 F. Supp. 3d at 609 (quoting *Kyllo v. United States*, 533 U.S. 27, 33 (2001)).

240. *See id.* at 609 (quoting *City of Ontario v. Quon*, 560 U.S. 746, 760 (2010)).

241. *See id.* at 609 (quoting *Kyllo*, 533 U.S. at 31).

242. *Id.* at 611; *see also* Jonathan Manes, *Secrecy & Evasion in Police Surveillance Technology*, 34 BERKLEY TECH. L.J., 503, 519 n.65 (2019).

243. *See Lambis*, 197 F. Supp. 3d at 611.

Department, witnesses identified Kerron Andrews as the shooter during a drug deal that turned sour.²⁴⁴ Based on the identifications, officers with the Baltimore City Police Department obtained an arrest warrant for Andrews.²⁴⁵ After the investigating officers could not locate Andrews, they obtained an order for a pen register and a trap-and-trace device on his cell phone in part because he knew about the arrest warrant and was hiding.²⁴⁶ After receiving information that indicated Andrews' general location, the officers used a Hailstorm, without a warrant, "to pinpoint the location of the cell phone as being inside the residence at 5032 Clifton Avenue."²⁴⁷

The police officers went to this residence and "found Andrews seated on the couch in the living room with the cell phone in his pants pocket" after gaining consensual entry inside.²⁴⁸ More importantly, they found a firearm in the couch cushions after obtaining a search warrant for this residence.²⁴⁹ Andrews' defense attorney filed a motion to suppress all evidence from this residence based on the police officers' use of the Hailstorm device.²⁵⁰ The trial court agreed with Andrews, finding that the use of the Hailstorm violated his Fourth Amendment right and thus any evidence in the residence must be suppressed.²⁵¹ Thus, while the arrest warrant was still valid, the evidence from the residence was the fruit of the poisonous tree.²⁵²

The prosecution appealed the decision to suppress this evidence pursuant to the Fourth Amendment. The Court of Special Appeals of Maryland also concluded that use of the Hailstorm constituted a search for purposes of the Fourth Amendment based on the trial court's factual record and the *Katz* reasonable expectation of privacy standard.²⁵³ Specifically, it held "that the use of a cell-site simulator, such as a Hailstorm, by the Government, requires a search warrant based on probable cause and describing with particularity the object and manner of the search."²⁵⁴

244. Civil No. CCB-16-2010, 2018 WL 3649602, at *1 (D. Md. Aug. 1, 2018); *see also* *State v. Andrews*, 134 A.3d 324, 327 (Md. App. 2016).

245. *See Andrews*, 134 A.3d at 327; *see also* Leonetti, *supra* note 235, at 689 (finding that the Baltimore Police Department had a warrant for Andrews' arrest).

246. *See Andrews*, 134 A.3d at 327; *Andrews v. Balt. City Police Dep't*, 2018 WL 3649602 at *1.

247. *Andrews*, 134 A.3d at 329; *see also Andrews v. Balt. City Police Dep't*, 2018 WL 3649602 at *2; Leonetti, *supra* note 235, at 689.

248. *Andrews*, 134 A.3d at 329; *Andrews v. Balt. City Police Dep't*, 2018 WL 3649602 at *2; *see also* Leonetti, *supra* note 235, at 689.

249. *See Andrews*, 134 A.3d at 329; *see also* Leonetti, *supra* note 235, at 689.

250. *See Andrews*, 134 A.3d at 330.

251. *See id.* at 333.

252. *See id.* at 333–34. The Supreme Court fashioned the "fruit of the poisonous tree" doctrine to limit the admissibility of evidence that was directly obtained by an invalid search. *See Wong Sun v. United States*, 371 U.S. 471, 485–88 (1963) (establishing the doctrine by name); *see also Silverthorne Lumber Co. v. United States*, 251 U.S. 385, 391–92 (1920) (holding that evidence improperly obtained shall not be used); *Nardone v. United States*, 308 U.S. 338, 341 (1939) (same).

253. *See id.* at 339–50; *see also* Leonetti, *supra* note 235, at 689–90.

254. *Andrews*, 134 A.3d at 350.

In affirming the suppression of the evidence, the appellate court further determined that the Maryland pen register statute did not authorize the police officers to use the Hailstorm.²⁵⁵ Moreover, the pen register order that the officers obtained did not substitute as a search warrant regarding the Hailstorm's use.²⁵⁶

Next, the District of Columbia appellate court also reached the conclusion that using a cell-site simulator constituted a search pursuant to the Fourth Amendment. Detective Rachel Pulliam of the Metropolitan Police Department in the District of Columbia was investigating two sexual assaults in which the assailant then robbed the victims of their cell phones and money.²⁵⁷ Both victims were escorts who told Detective Pulliam that their attacker had called them on their cell phones.²⁵⁸ After comparing the cell phone logs from both victims and identifying a common cell number, Detective Pulliam sought assistance from Sergeant Todd Perkins in the Technical Services Unit.²⁵⁹

Initially, Sergeant Perkins sought the targeted cell phone's subscriber information but failed because it was a prepaid cell phone without such information.²⁶⁰ Moreover, he sought location information from the relevant telecommunication providers, which was updated every fifteen minutes.²⁶¹ By reviewing the location data for both the suspect's cell phone and one of the victim's cell phones, Sergeant Perkins determined that the cell phones were near the Minnesota Avenue Metro Station.²⁶²

With the information about the general vicinity of the cell phones, Sergeant Perkins drove a truck with a cell-site simulator to that station.²⁶³ Based on the data provided by the cell-site simulator, the officers located Jones inside a parked car at the station with his girlfriend.²⁶⁴ They arrested Jones, recovering evidence including a weapon and the victims' cell phones.²⁶⁵

At a suppression hearing, Sergeant Perkins testified about how cell-site simulators work.²⁶⁶ Jones called an expert from the telecommunications industry about cell phone networks and systems, who testified that an active cell-site simulator allows an officer to obtain a cell phone's unique identifiers, such as the IMSI number, as well as the locational direction of the targeted cell phone and how far it is

255. See *id.* at 355.

256. See *id.* at 360–61.

257. See *Jones v. United States*, 168 A.3d 703, 707–08 (D.C. 2017); see also Harvey Gee, *Almost Gone: The Vanishing Fourth Amendment's Allowance of Stingray Surveillance in a Post-Carpenter Age*, 28 BERKLEY TECH. L.J. S. CAL REV. L. & SOC. JUST. 409, 440 (2019).

258. See *Jones*, 168 A.3d at 707.

259. See *id.* at 708.

260. See *id.*

261. See *id.*

262. See *id.*

263. See *id.*; see also Gee, *supra* note 257, at 440.

264. See *Jones*, 168 A.3d at 709.

265. See *id.*

266. See *id.*

from a cell-site simulator.²⁶⁷ The trial court found that there were no exigent circumstances justifying the cell-site simulator's use as the police officers had time to obtain a warrant.²⁶⁸ However, the court determined that the inevitable discovery doctrine applied because the officers would have located Jones through the cell-site simulator's location of the victim's cell phone.²⁶⁹

On appeal, the District of Columbia Court of Appeals determined "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."²⁷⁰ Next, the appellate court addressed whether the inevitable discovery doctrine applied.²⁷¹ It concluded that the evidence that Sergeant Perkins switched to tracking the victim's cell phone with the cell-site simulator might establish that the police officers *could* have apprehended Jones and the incriminating evidence separate and apart from the invalid search.²⁷² However, that possibility does not establish that they would have done so such that the discovery was inevitable which is the appropriate legal standard.²⁷³ Thus, the court found the incriminating evidence inadmissible based on the inevitable discovery doctrine.²⁷⁴

The appellate court also addressed whether the incriminating evidence was admissible pursuant to the good-faith exception to the exclusionary rule.²⁷⁵ Not only were these police officers acting without a warrant, but there was no statute or judicial decision justifying their search based on "a secret technology that they had shielded from judicial oversight and public scrutiny."²⁷⁶ Thus, the good-faith exception did not apply to the incriminating evidence obtained during Jones's arrest.²⁷⁷

Finally, the appellate court determined that the incriminating statements that Jones made after the police officers located him constituted the fruit of the poisonous tree.²⁷⁸ Additionally, evidence obtained from the purse of the girlfriend who was in the car was also fruit of the poisonous tree.²⁷⁹ Thus, the court excluded all

267. *See id.* at 709–10.

268. *See id.* at 710–11.

269. *See id.* at 711.

270. *See id.* at 713; *see also* United States v. Powell, No. 2:18-cv-13107, 2020 WL 3868500, at *4 (E.D. Mich. July 9, 2020) (citing *Jones*, 168 A.3d at 711–13) ("The use of a cell site simulator to track or locate a person likely constitutes a 'search' and requires a warrant."), *appeal filed*, No. 20-1894 (6th Cir. Sept. 17, 2020); Manes, *supra* note 242, at 518 n.63.

271. *See Jones*, 168 A.3d at 717–19. In *Nix v. Williams*, 467 U.S. 431 (1984), the Supreme Court established the inevitable discovery doctrine by which evidence may be admissible when that evidence is discovered during a warrantless or otherwise improper search if the evidence would have been obtained by some other manner of investigation that is untainted from the original invalid search.

272. *See Jones*, 168 A.3d at 718.

273. *See id.*

274. *See id.* at 718–19.

275. *See id.* at 719–20.

276. *See id.* at 720.

277. *See id.*

278. *See id.* at 722.

279. *See id.* at 722–23.

of this incriminating evidence because law enforcement failed to obtain a search warrant prior to their use of a cell-site simulator, and none of the exceptions to the exclusionary rule applied.²⁸⁰

Finally, a California federal district court determined that using a cell-site simulator constituted a search pursuant to the Fourth Amendment. In *United States v. Ellis*,²⁸¹ during the course of an investigation into a shooting of a police officer, the Oakland Police Department and the FBI used cell-site simulators to track and locate Purvis Ellis's cell phone.²⁸² They located him in his apartment complex building the morning after the shooting.²⁸³ Neither the FBI nor the Oakland Police Department sought a search warrant authorizing the cell-site simulator use but instead only obtained an order from a state court judge authorizing a pen register and a trap-and-trace device.²⁸⁴

In discussing whether there was a search based on the use of the cell-site simulator, the *Ellis* court explained that there are two approaches to establishing a search. First, there is the traditional property-centric trespass approach revitalized by the Supreme Court in *Jones*.²⁸⁵ Second, a search can be established under the "reasonable expectation of privacy" test enunciated in *Katz*.²⁸⁶

Ellis argued that he suffered a Fourth Amendment violation when the cell-site simulators' signals penetrated the walls of his home.²⁸⁷ Because the record before the trial court was insufficient as to whether Ellis was actually in his home when law enforcement officers deployed the cell-site simulator, the trial court did not make any determination of this claim.²⁸⁸

Next, the *Ellis* court addressed the "reasonable expectation of privacy" test, finding that Ellis established "that the use of the Stingray devices amounted to a search in violation of a reasonable expectation of privacy in the real-time location of his cell phone."²⁸⁹ Moreover, it held that using the cell-site simulator constituted a search within the meaning of the Fourth Amendment that necessitated a warrant absent any exceptions.²⁹⁰ Additionally, the order authorizing the use of a pen register and trap-and-trace device was inadequate to meet the constitutional standard for the use of the cell-site simulators.²⁹¹ Unfortunately for Ellis, the court determined that exigent circumstances existed for a warrantless search,²⁹² that the

280. See *id.* at 722–26.

281. 270 F. Supp. 3d 1134 (N.D. Cal. 2017).

282. See *id.* at 1139.

283. See *id.* at 1141.

284. See *id.* at 1147.

285. See *id.* at 1139 (discussing *United States v. Jones*, 565 U.S. 400, 404–05 (2012)).

286. See *id.* at 1139–40 (discussing Justice Harlan's concurrence in *Katz v. United States*, 389 U.S. 347, 361 (1967)).

287. See *id.* at 1140.

288. See *id.* at 1141.

289. *Id.* at 1141–42.

290. See *id.* at 1145–46.

291. See *id.* at 1148–49.

292. See *id.* at 1149–53.

Fourth Amendment's good-faith exception applied,²⁹³ and that the inevitable-discovery doctrine precluded suppression.²⁹⁴

C. Some Courts Analyze Cell-Site Simulator Decisions Based on the Assumption that a Search Warrant is Necessary

In two decisions issued by the Florida District Court of Appeals, the court did not directly address whether using a cell-site simulator constitutes a search.²⁹⁵ Instead, the court implicitly established that there is a search because law enforcement had to obtain a warrant based upon probable cause before using a cell-site simulator.²⁹⁶

In *State v. Sylvestre*,²⁹⁷ police officers investigated an armed robbery and a murder at a Boca Raton restaurant.²⁹⁸ During the course of this investigation, they obtained a court order authorizing them to obtain cell site location information for a cell phone associated with Quinton Sylvestre.²⁹⁹ Specifically, the order mandated that the telecommunications provider "disclose 'all cell-site activations and sectors for all incoming and outgoing calls/communications ... call detail location records, 'angle from the tower' data, including [those] contemporaneous (real-time) with these communications, and historical calls/communications detail records.'"³⁰⁰ Moreover, the trial court also issued an order authorizing pen register and trap-and-trace device.³⁰¹ After the officers used the cell-site simulator to pinpoint Sylvestre's location, they then obtained a search warrant for his home.³⁰²

Sylvestre filed a motion to suppress all evidence obtained from his home, arguing that law enforcement officers exceeded the scope of the warrant for the cell site location information, when they used the cell-site simulator.³⁰³ At the hearing, a sergeant with the Broward County Sheriff's Department testified that the order did not provide for any GPS locations, but instead only tower data.³⁰⁴ Because they could only locate Sylvestre's cell phone within a general vicinity of about several square blocks, they used a cell-site simulator.³⁰⁵ Sylvestre's expert also testified "that, at best, the CSLI order could provide general location information, which would only be accurate for several square blocks of a particular area."³⁰⁶

293. *See id.* at 1153–57.

294. *See id.* at 1157–58.

295. *State v. Sylvestre*, 254 So. 3d 986 (Fla. Dist. Ct. App. 2018); *State v. Martin*, 287 So. 3d 645 (Fla. Dist. Ct. App. 2019) (per curiam).

296. *Sylvestre*, 245 So. 3d at 991–92; *Martin*, 287 So. 3d at 648–49.

297. 254 So. 3d 986.

298. *See id.* at 987.

299. *See id.* at 987.

300. *Id.* at 988.

301. *See id.*

302. *See id.*

303. *See id.*

304. *See id.*

305. *See id.*

306. *Id.*

Moreover, the expert emphasized that “[o]nly a cell-site simulator could provide the State the exact location of the Defendant’s cell phone.”³⁰⁷ The trial court suppressed the evidence from Sylvestre’s home because “of the warrantless use of the cell-site simulator.”³⁰⁸

On appeal, the prosecution argued that the trial court erred “because (1) the CLSI Order permitted the use of a cell-site simulator, and (2) the State did not have to disclose its intention to use a cell-site simulator.”³⁰⁹ Analyzing a number of recent Supreme Court decisions regarding cell phones, the court determined that, based on *Riley* and *Carpenter*, law enforcement cannot use technological devices to search for a cell phone in an individual’s possession absent a search warrant.³¹⁰ The appellate court did not fully address whether using a cell-site simulator constituted a search. However, the court implicitly reached that conclusion because it held that before using such a device the government must obtain a warrant based on probable cause.³¹¹

In *State v. Martin*,³¹² the same Florida state appellate court considered a similar appeal in which the trial court granted a motion to suppress when law enforcement used a cell-site simulator without a warrant.³¹³ Martin’s mother was found dead in the apartment that he shared with her, leading to a murder charge against him.³¹⁴ Police officers used a cell-site simulator to track Martin and found him in the victim’s car with incriminating evidence.³¹⁵ The trial court granted Martin’s motion to suppress this evidence based on the Fourth Amendment.³¹⁶

On appeal, the prosecution argued that the trial court erred in finding that Martin had standing to challenge the search using the cell-site simulator.³¹⁷ The appellate court rejected this argument finding that Martin indeed had standing.³¹⁸ As in *Sylvestre*, the court did not directly address the question of whether the cell-site simulator usage constitutes a Fourth Amendment search, but instead, it was implicit within the court’s overall reasoning.

307. *Id.*

308. *Id.*

309. *Id.* at 989.

310. *See id.* at 991–92 (discussing *Riley v. California*, 573 U.S. 373 (2014), and *Carpenter v. United States*, 585 U.S. ___, 138 S. Ct. 2206 (2018)).

311. *See id.*; *see also In Re United States for an Ord. Relating to Telephones Used by Suppressed*, No. 15 M 0021, 2015 WL 6871289, at *3 (N.D. Ill. Nov. 9, 2015) (unpublished) (acknowledging implicitly the necessity of a search as “there is no dispute that a warrant meeting the probable cause standard is necessary to use a cell-site simulator” to locate a pre-paid cell phone used in a drug trafficking enterprise).

312. 287 So. 3d 645 (Fla. Dist. Ct. App. 2019) (per curiam).

313. *See id.* at 646.

314. *See id.*

315. *See id.*

316. *See id.*

317. *See id.* at 647.

318. *See id.*

In *United States v. Artis*,³¹⁹ the Ninth Circuit reviewed a decision by the United States District Court for the Northern District of California which had assumed that the Government needed to obtain a warrant.³²⁰ The FBI began investigating Donnell Artis and Chanta Hopkins for identity theft and credit card fraud.³²¹ Both suspects were fugitives based on outstanding state arrest warrants.³²² An FBI agent filed an application seeking authorization to use a cell-site simulator to track the location of Hopkins's cell phone, asserting that Hopkins was a fugitive.³²³ A state court judge issued a search warrant authorizing the use of a cell-site simulator by county law enforcement officers along with United States Marshals.³²⁴ Based in part on the use of the cell-site simulator, agents apprehended Hopkins outside his San Francisco apartment and arrested him.³²⁵

The defendants filed motions to suppress the evidence obtained based in part on the use of the cell-site simulator.³²⁶ After an evidentiary hearing, the trial court granted both motions to suppress, finding that neither warrant approving the use of a cell-site simulator was supported by probable cause.³²⁷

On appeal, the United States Court of Appeal for the Ninth Circuit indicated that it would "assume (as the government has) that use of a cell-site simulator to track the location of Hopkins's cell phone . . . required a warrant."³²⁸ The court noted that as the searches were conducted pursuant to warrants, Hopkins had to establish that his warrant was invalid pursuant to the Fourth Amendment, or, if valid, then "executed in a manner that rendered the search[] unreasonable."³²⁹ The Ninth Circuit determined that there was probable cause to support the search warrant authorizing the use of a cell-site simulator to locate Hopkins's cell phone because the agent demonstrated that Hopkins was a fugitive from justice.³³⁰

D. In Some Prosecutions, the Government Has Conceded That a Search Warrant Was Necessary to Use a Cell-Site Simulator

Some courts have addressed law enforcement's use of a cell-site simulator without a warrant in a context in which the prosecution conceded that this usage constituted a search.

319. 919 F.3d 1123 (9th Cir. 2019).

320. See generally *United States v. Artis*, 315 F. Supp. 3d 1142 (N.D. Cal. 2018) (acknowledging implicitly the necessity of obtaining a warrant).

321. See *Artis*, F.3d at 1126.

322. See *id.*

323. See *id.* at 1127.

324. See *id.*

325. See *id.* at 1128.

326. See *id.*

327. See *id.*; *United States v. Artis*, 315 F. Supp. 3d 1142, 1145 (N.D. Cal. 2018).

328. *Artis*, 919 F.3d at 1128.

329. See *id.*

330. See *id.* at 1134–35.

There was a valid arrest warrant for Damian Patrick based on parole violations regarding his state court conviction.³³¹ Officers with the Milwaukee Police Department also obtained another warrant authorizing them to locate Patrick based on his cell phone data.³³² Using a cell-site simulator, police officers located and arrested Patrick in his car on a public street.³³³ Because Patrick possessed a firearm at the time of his arrest, the federal government indicted him for being a felon in possession of a firearm, pursuant to 18 U.S.C. § 922(g)(1).³³⁴

Patrick filed a motion to suppress evidence of the firearm. A federal magistrate judge issued a report and recommendation that the motion be denied, and the district court adopted it.³³⁵ On appeal to the United States Court of Appeals for the Seventh Circuit, the court noted that the question of whether the use of the cell-site simulator constituted a search for purposes of the Fourth Amendment was an open one.³³⁶ This appellate court did not address the issue because “[t]he United States . . . conceded for the purpose of this litigation that use of a cell-site simulator is a search”³³⁷

The dissent chastised the Government for “appear[ing] to have purposefully concealed the Stingray’s use from the issuing magistrate, the district court, defense counsel, and even this court. It ultimately admitted its use of the device only in response to an *amicus curiae* brief filed during this appeal.”³³⁸ Ultimately, the Seventh Circuit held that the exclusionary rule did not mandate that evidence obtained in this case based on the use of a cell-site simulator be excluded.³³⁹

Similarly, in an appeal to Maryland’s highest court, the prosecution conceded that the use of the cell-site simulator constituted a search.³⁴⁰ In *State v. Copes*, Baltimore detectives were investigating the murder of a homeless woman, including a lead that the cell phone she had was missing.³⁴¹ They sought to locate two

331. See *United States v. Patrick*, 842 F.3d 540, 542 (7th Cir. 2016).

332. See *id.* at 542.

333. See *id.* at 541, 542.

334. See *id.* at 541.

335. See *id.* at 541; see also *United States v. Patrick*, No. 13-CR-234, 2015 WL 106158 at *1 (E.D. Wis. Jan. 7, 2015) (unpublished) (adopting magistrate judge’s report and recommendation).

336. See *Patrick*, 842 F.3d at 543; see also Manes, *supra* note 243, at 519 n.66.

337. *Patrick*, 842 F.3d at 544; see also *State v. Tate*, 849 N.W.3d 798, 801 (Wis. 2014) (Supreme Court of Wisconsin assumed without deciding that law enforcement’s use of a cell-site simulator to locate the suspect in his mother’s home constituted a search for purposes of the Fourth Amendment.); *United States v. Rigmaiden*, 844 F. Supp. 2d 982, 995–96 (D. Ariz. 2012) (Federal prosecutor indicated that “for purposes of Defendant’s motion to suppress, . . . the Court may assume that the aircard tracking operation was a Fourth Amendment search and seizure.”).

338. *Patrick*, 842 F.3d at 546 (Wood, J., dissenting); see also Manes, *supra* note 242, at 512 n.29.

339. See *Patrick*, 842 F.3d at 545. In a dissenting opinion, Chief Judge Diana Wood argued that the record was inadequate to address whether the use of the Stingray “was sufficiently outside the scope of the warrant to merit blanket suppression,” especially in light of the government’s attempts to prevent information about the device from reaching the public, including the agreement “to dismiss cases rather than disclose use of Stingray.” *Id.* at 546 (Wood, J., dissenting).

340. See *State v. Copes*, 165 A.3d 418, 431 (Md. 2017).

341. See *id.* at 421.

cell phones associated with the victim in hopes that it would further the murder investigation.³⁴²

These detectives then obtained a court order authorizing the use of a cell-site simulator pursuant to the established Baltimore City Police Department procedure of applying to use a pen register and trap-and-trace device.³⁴³ In the pen register application, the detective asserted there was probable cause to believe that the missing cell phones would have been taken by potential suspects and subsequently used by the potential suspects while service is still connected.³⁴⁴ Significantly, the trial court authorized the investigators “to ‘employ . . . [a] Cellular Tracking Device [and] initiate a signal to determine the location of the subject’s mobile device on the service provider’s network or with such other reference points as may be reasonably available, Global Position System Tracing and Tracking, Mobile Locator tools, R.T.T. (Real Time Tracking Tool).’”³⁴⁵

Based on cell site location information, the detectives determined that the missing cell phone was in a specific Baltimore neighborhood.³⁴⁶ After deploying the cell-site simulators in that neighborhood, the devices indicated that the victim’s cell phone was in an apartment building across the street from where her body was found.³⁴⁷ The detective knocked on the apartment door of Robert Copes, who was recognizable from video surveillance photos in part because of his distinctive blue and yellow coat.³⁴⁸ The investigators then obtained a search warrant for his apartment which led to additional incriminating information against Copes.³⁴⁹

After the grand jury indicted Copes, he filed a motion to suppress all the evidence obtained from his apartment and his statements to the police.³⁵⁰ The trial court granted the motion to suppress based largely on the recent appellate court decision in *Andrews*,³⁵¹ notwithstanding its determination that the investigators acted in good faith.³⁵² The prosecution appealed this decision, but the appellate court affirmed based on *Andrews*, finding in part that the officers did not act in good faith because they failed to adequately describe the device they were seeking to use pursuant to the pen register application.³⁵³

The *Copes* court first noted that the issues before it first concerned whether the use of the cell-site simulator constituted a search pursuant to the Fourth

342. See *id.* at 426.

343. See *id.* at 423.

344. See *id.* at 426.

345. *Id.* at 427.

346. See *id.*

347. See *id.* at 428.

348. See *id.*

349. See *id.* at 428–29.

350. See *id.* at 429.

351. See *id.* at 430.

352. See *Copes*, 165 A.3d at 430.

353. See *id.* at 430–31.

Amendment.³⁵⁴ The court declined to directly address this question because “the State has conceded, for purposes of this case, that the use of the cell site simulator constituted a search.”³⁵⁵ In other words, it was generally accepted by the prosecution and the Court that the use of the cell-site simulator constituted a search. Ultimately, the *Copes* court reversed the trial court’s suppression of evidence, finding that the detectives’ conduct met the standard for the good-faith exception.³⁵⁶

Although the Supreme Court has not yet addressed cell-site simulators in a decision, in *Carpenter*, which instead concerned cell site location information, the Court determined that historical data about location was protected by the Fourth Amendment.³⁵⁷

Several state and federal courts have addressed the Fourth Amendment implications of cell-site simulators. Indeed, one federal judge noted that federal law enforcement officers “have settled into a practice of the government showing probable cause” for authorization to use a cell-site simulator.³⁵⁸ Regardless of the various contexts in which these courts discuss cell-site simulators, it is apparent that they view using them as a search.

V. LAW ENFORCEMENT OFFICIALS’ USE OF CELL-SITE SIMULATORS TO CONDUCT MASS SURVEILLANCE VIOLATES THE FOURTH AMENDMENT AS A GENERAL WARRANT

In discussing the three circumstances in which law enforcement officials use cell-site simulators, the most aggressive involves deploying the device on random targets, including on individuals at protests.³⁵⁹ This scenario is a fishing expedition by law enforcement searching for potential criminal conduct. In *Berger v. New York*, the Supreme Court held as unconstitutional a New York law that authorized eavesdropping on telephone calls because it did not “require[] belief that any particular offense has been or is being committed; nor that ‘property’ sought, the conversations, be particularly described.”³⁶⁰ Thus, *Berger* required that there be probable cause that a crime occurred.³⁶¹ In *City of Indianapolis v. Edmond*, the Court held that a generalized approach to law enforcement violates the Fourth Amendment.³⁶² Moreover, the *Edmond* Court struck down the Indianapolis

354. *See id.* at 431.

355. *Id.*

356. *See id.* at 447.

357. *Carpenter v. United States*, 585 U.S. ___, 138 S. Ct. 2206, 2217–18 (2018).

358. James Orenstein, *Judicial Engagement with Surveillance Technology*, 49 CONN. L. REV. 1717, 1726 (2017).

359. *See supra* Section IV.B.

360. *Berger v. New York*, 388 U.S. 41, 58–59 (1967).

361. *Id.* at 59.

362. *City of Indianapolis v. Edmond*, 531 U.S. 32, 44 (2000) (“We cannot sanction stops justified only by the generalized and ever-present possibility that interrogation and inspection may reveal that any given motorist has committed some crime.”).

ordinance because the checkpoints were essentially designed for general crime control and thus violated the Fourth Amendment.³⁶³

There are reports around the country that law enforcement's usage of cell-site simulators function as general warrants and therefore violate the Fourth Amendment. As early as 2007, it is believed that federal law enforcement agencies used cell-site simulators in airplanes to conduct mass surveillance: "The technology in the two-foot-square [dirtbox] device enables investigators to scoop data from tens of thousands of cellphones in a single flight, collecting their identifying information and general location."³⁶⁴ Thus, law enforcement has used cell-site simulators in a generalized manner in support of suspicionless attempts to collect as much data as possible from members of the public.

Even earlier than 2007, law enforcement officials were using cell-site simulators to monitor protestors' cell phones. In 2003, the Miami-Dade Police Department submitted an emergency request to upgrade its Triggerfish surveillance by purchasing StingRay and Amberjack devices to use during the Free Trade Area of the Americas Conference in November of that year.³⁶⁵ The request specifically explained that accessing cell phone data provides valuable information to law enforcement:

Based on the history of these conferences, the department anticipated criminal activities directed at attendees and conference sites facilitated by the use of cellular phones. Wireless phone tracking systems utilized by law enforcement have proven to be an invaluable tool in both the prevention of these offenses and the apprehension of individuals attempting to carry out criminal activities.³⁶⁶

In other words, the Miami-Dade police candidly acknowledged that it wanted to use the StingRay and Amberjack to surveil protestors at the conference.

Other police departments have seemingly followed Miami's lead, although with less candor about their goals. Although law enforcement does not announce that it has engaged in such types of use regarding cell-site simulators, there is anecdotal evidence of such usage.

363. *See id.* at 48.

364. Devlin Barrett, *Americans' Cellphones Targeted in Secret U.S. Spy Program*, WALL STREET JOURNAL (Nov. 12, 2014, 8:22 PM), <https://www.wsj.com/articles/americans-cellphones-targeted-in-secret-u-s-spy-program-1415917533>; *see also* Owsley, *supra* note 176, at 81-82 (finding that the use of dirtboxes is analogous to warrantless searches using a cell-site simulator).

365. Cyrus Farivar, *Powerful 'stingrays' used to go after 911 hangup, ATM burglary*, ARS TECHNICA (Feb. 25, 2015, 7:45 AM), <https://arstechnica.com/tech-policy/2015/02/powerful-stingrays-used-to-go-after-911-hangup-atm-burglary/>; MIAMI DADE POLICE DEPARTMENT, SECTION 5 EMERGENCY PURCHASES, 5-1, Bid Number E1715-PD (2003), <https://www.documentcloud.org/documents/1675293-miami-dade.html>.

366. *Id.*

A. New York

During a December 2014 protest in New York City by Millions March NYC, which is associated with the Movement for Black Lives regarding the killings of Michael Brown and Eric Garner, activist Vienna Rye's "cell phone shut down during the march while she was trying to film what was happening."³⁶⁷ Ms. Rye further asserted in her petition against the New York Police Department that her "phone indicated that it was out of battery power even though it was fully charged."³⁶⁸

Moreover, in April 2015, Ms. Rye and her co-petitioners Arminta Jeffryes and Nabil Hassein all experienced problems with their cell phones while protesting the killing of Freddie Gray in New York City.³⁶⁹ Additionally, in April 2016, both Ms. Jeffryes and Ms. Rye "lost reception on their cell phones for no apparent reason" during a protest at the New York State Republican Committee's annual gala in Manhattan.³⁷⁰

Not only does the New York Police Department have cell-site simulators, but it has admitted "that it had used Stingray technology more than a thousand times between 2008 and 2015" to investigate a variety of criminal offenses.³⁷¹ In this context, Ms. Rye, Ms. Jeffryes, and Mr. Hassein filed a state Freedom of Information Law ("FOIL") claim against the New York Police Department seeking, among other information, whether it used cell-site simulators against protestors.³⁷²

Although the New York Police Department objected to providing any response to the petitioners, the trial court noted that the lawsuit "arises from reports of protestors who claim that their cellphones are suddenly unable to function while in the middle of a protest. That possibility, that [the New York Police Department] is interfering with protestors' ability to communicate with each other, is a serious concern ripe for the use of FOIL."³⁷³ The judge rejected the New York Police Department's concerns ordering it to confirm or deny whether records about what

367. *In re Millions March N.Y.C. v. N.Y.P.D.*, No. 100690/2017, Am. Opening Mem. of Law in Support of Verified Pet., at 3 (N.Y. Sup. Ct. Oct. 5, 2018); Ali Winston, *Did the Police Spy on Black Lives Matter Protestors? The Answer May Soon Come Out*, N.Y. TIMES (Jan. 14, 2019).

368. *In re Millions March N.Y.C. v. N.Y.P.D.*, No. 100690/2017, Am. Opening Mem. of Law in Support of Verified Pet., at 3 (N.Y. Sup. Ct. Oct. 5, 2018). This disruption of a cell phones features is reported by protestors in other parts of the country. For example, people protesting in Ferguson, Missouri after the killing of Michael Brown complained that their cell phones would drop calls and make unusual tones or clicks when used. See Lussenhop, *supra* note 161.

369. *In re Millions March N.Y.C. v. N.Y.P.D.*, No. 100690/2017, Am. Opening Mem. of Law in Support of Verified Pet., at 3 (N.Y. Sup. Ct. Oct. 5, 2018).

370. *Id.*

371. Winston, *supra* note 267.

372. See *In re Millions March N.Y.C. v. N.Y.P.D.*, No. 100690/2017, Am. Opening Mem. of Law in Support of Verified Pet., at 1–2 (N.Y. Sup. Ct. Oct. 5, 2018); Winston, *supra* note 367.

373. *In re Millions March N.Y.C. v. N.Y.P.D.*, No. 100690/2017, Decision and Order, at 6 (N.Y. Sup. Ct. Jan. 11, 2019).

it does to the protestors' cell phones during protests simply exist.³⁷⁴ Based on this court order, the New York Police Department then indicated that it had no records of cell phone surveillance during the Millions March NYC protest.³⁷⁵

B. Chicago

During a late November 2014 protest in Chicago regarding the police killing of Eric Garner and Michael Brown, hackers with the group "Anonymous" reportedly obtained a radio exchange on a police scanner involving a police officer asking whether there was any monitoring of some protestors:

Dispatch: "CPIC [Chicago police's spy 'fusion' center] on the air for a mobile."

Officer 1: "Go ahead."

Officer 2: "Yeah one of the girls, an organizer here, she's been on her phone a lot. You guys picking up any information, uh, where they're going, possibly?"

Officer 1: "Yeah we'll keep an eye on it, we'll let you know if we hear anything."

Officer 2: "10-4. They're compliant, and they're, they're doing ok now but she's spending a lot of time on the phone."

Officer 1: "10-4."³⁷⁶

It appears that Officer 2 is asking others in CPIC to access this woman's cell phone.³⁷⁷ The officers targeted Kristiana Rae Colón, the protest organizer. She caught the attention of the police officer on the scene.³⁷⁸ Indeed, someone attending this protest videoed a police vehicle equipped with a cell-site simulator.³⁷⁹ In response to the officer at the scene of this protest, an officer indicated, "Bill, I want to give you a call on your cell."³⁸⁰ Ms. Colón reported that Commander William

374. *Id.* at 7, 12–13.

375. Liam Knox, *NYPD, told it can't use 'Glomar' denial, now claims it has not records on Millions March cell phone surveillance*, MUCKROCK (Mar. 21, 2019), <https://www.muckrock.com/news/archives/2019/mar/21/css-nypd-glomar/>.

376. *Activists Say Chicago Police Used 'Stingray' Eavesdropping Technology During Protests*, CBS CHICAGO (Dec. 6, 2014, 11:19 AM), <https://chicago.cbslocal.com/2014/12/06/activists-say-chicago-police-used-stingray-eavesdropping-technology-during-protests/>; Patrick Smith, *Lawsuit seeks information on alleged CPD spying*, WBEZ (Dec. 8, 2014, 2:33 PM), <https://www.wbez.org/stories/lawsuit-seeks-information-on-alleged-cpd-spying/03b8cb91-1c28-48dd-b89e-f41149f09606>; *LOOKS LIKE CHICAGO PD HAD A STINGRAY OUT AT THE ERIC GARNER PROTEST LAST NIGHT*, PRIVACY SOS BLOG (Dec. 8, 2014), <https://privacysos.org/blog/looks-like-chicago-pd-had-a-stingray-out-at-the-eric-garner-protest-last-night/>; *see also* Boyle v. City of Chicago, No. 17-cv-00244, Jerry Boyle Dep., at 18 (N.D. Ill. Aug. 22, 2017) (referencing this incident).

377. *See* Rachel Anspach, *Evidence Strongly Suggests CPD Illegally Uses Stingray Technology on Protestors*, GAPERS BLOCK (Jan. 12, 2015), <http://gapersblock.com/mechanics/2015/01/12/evidence-suggests-cpd-illegally-uses-stingray-technology-on-protestors/>.

378. *See id.*

379. *LOOKS LIKE CHICAGO PD HAD A STINGRAY OUT AT THE ERIC GARNER PROTEST LAST NIGHT*, PRIVACY SOS BLOG (Dec. 8, 2014), <https://privacysos.org/blog/looks-like-chicago-pd-had-a-stingray-out-at-the-eric-garner-protest-last-night/>.

380. Anspach, *supra* note 377.

Dunn was following her during the protest.³⁸¹ Commander Dunn's conduct influenced other Chicago activists, including Jerry Boyle, to engage in counter-surveillance of police regarding their use of this technology.

The recording from the police scanner about the police surveillance of Ms. Colón during this November 2014 protest confirmed the types of allegations asserted by Freddy Martinez, an activist who has sued the City of Chicago for information about the police department's use of cell-site simulators.³⁸² Specifically, he noticed at protests as early as 2012 that cell phone "batteries were burning quickly, and messages were not getting through, which seems very consistent with Stingray behavior."³⁸³ When law enforcement deploys cell-site simulators, this type of adverse impact on cell phones is a possible occurrence.³⁸⁴

Moreover, Mr. Martinez has had experience with Chicago police surveillance vehicles. At a February 2014 protest, he used a cell phone app that enabled him to see the locations of all nearby cell towers.³⁸⁵ Interestingly, the app revealed a cell tower that was actually moving towards him as a police vehicle arrived.³⁸⁶ He explained that after seeing "an unmarked Chicago police green license plate" on the vehicle, he and other activists "then . . . saw a cell phone tower broadcast, and . . . thought it was some kind of surveillance device."³⁸⁷ In light of this "suspicious" development, Mr. Martinez concluded that the cell tower "seemed to be the car itself."³⁸⁸

On January 15, 2015, Jerry Boyle, an attorney, volunteered as a legal observer from the National Lawyers Guild for a "Reclaim MLK Day" event in Chicago during which he alleged Chicago police officers targeted his cell phone with a cell-site simulator.³⁸⁹ After hearing Commander Bill Dunn request CPIC to spy on Ms. Colón's cell phone less than two months earlier, he was prepared.³⁹⁰ Before attending that protest, Mr. Boyle installed the OpenSignal app on his cell phone with the intention of using it to determine whether the Police Department was using

381. *See id.*

382. *See* Martinez v. Cook Cnty. State's Atty's Off., 103 N.E.3d 351 (Ill. App. Ct. 2018).

383. Anspach, *supra* note 377.

384. *See* Zetter, *supra* note 141 ("Because a stingray is not really a tower on the carrier's network, calls and messages to and from a phone can't go through while the phone is communicating with the stingray.").

385. *See* Anspach, *supra* note 377.

386. *See id.*

387. *See id.*

388. *See id.*

389. Cyrus Farivar, *Lawyer sues Chicago police, claims they used stingray on him*, ARS TECHNICA (Jan. 13, 2017, 8:04 AM), <https://arstechnica.com/tech-policy/2017/01/lawyer-sues-chicago-police-claims-they-used-stingray-on-him/>.

390. Boyle Dep., *supra* note 376, at 61; *see also id.* at 75 ("[A]fter that incident on Black Friday in 2014, we formed, you know, I'm calling it a working group, but a group of us got together both online and sometimes in person to discuss how we deal with it.").

cell-site simulators.³⁹¹ While monitoring the event, this app indicated that there was a cell tower in the middle of the street.³⁹²

Boyle and another National Lawyers Guild colleague at the rally took screenshots of the OpenSignal source as well as pictures of the police vehicle before it drove away.³⁹³ After the vehicle drove away, they then relaunched the OpenSignal app to determine where the cell-site simulator indicated by the app and the physical location of the police vehicle that they observed merged. When they relaunched the app, it then indicated that the cell tower was no longer located where the police car was.³⁹⁴ This second test confirmed for him that the police were using cell-site simulators.³⁹⁵ Specifically, it demonstrated the vehicle contained a cell-site simulator because the app no longer reported the device in that location once the police vehicle left.

Sometime after the incident in which the OpenSignal app indicated to Boyle that there was a cell tower in the middle of a street where a Chicago police vehicle was, he had another similar experience. Specifically, he explained that during an event in Grant Park, he saw some Chicago police vehicles, which raised his suspicions.³⁹⁶ Again, he used the OpenSignal app, which “showed a cell tower in the park somewhere . . . [even though] there’s no cell tower there.”³⁹⁷ As in the previous example, the app indicated the presence of cell-site simulators when the police vehicles were present but no longer noted the existence of the devices after the vehicles departed.

C. Baltimore

In Baltimore, large groups of protestors marched after the death of Freddie Gray in April 2015. In response, law enforcement engaged in significant surveillance efforts, including in the air. The American Civil Liberties Union posited that federal law enforcement agencies were flying surveillance planes over Baltimore after a Cessna was discovered flying a similar pattern repeatedly.³⁹⁸ The FBI denied that

391. *Id.* at 34; *see also id.* at 82–83 (describing the OpenSignal app as showing the app user all nearby cell towers).

392. *Id.* at 35, 93–94; *see also id.* at 48 (“[W]e had a result of OpenSignal showing that our phone was getting spied on.”).

393. *Id.* at 83–86, 97–98.

394. *Id.* at 93–97.

395. *Id.* at 86, 98.

396. *Id.* at 100–01.

397. *Id.* at 100.

398. Jay Stanley, *Mysterious planes over Baltimore spark surveillance suspicions*, MSNBC (May 6, 2016, 5:34 PM), <https://www.msnbc.com/msnbc/mysterious-planes-over-baltimore-spark-surveillance-suspicions-msna590236>; *see generally* Laura Moy, *Yet Another Way the Baltimore Police Unfairly Target Black People*, SLATE (Aug. 18, 2016), <https://slate.com/technology/2016/08/baltimore-police-use-surveillance-technology-to-target-black-neighborhoods.html> (“Baltimore . . . is a city where, through use of suitcase-size fake cellphone towers that can be used to track Baltimore residents, police disrupt the cellphone network on a regular basis, disproportionately—unfairly—focusing on black neighborhoods.”).

its aerial surveillance over Baltimore during these protests involved the use of cell-site simulators.³⁹⁹

Notwithstanding the denial by the FBI regarding the use of cell-site simulators during the Freddie Gray protests, the Baltimore Police Department has a history of extensive use of such devices.⁴⁰⁰ Baltimore Police Lieutenant Michael Fries testified before the Maryland State Senate that “Obviously, we probably use the [cell-site simulator] equipment more than anybody, in total.”⁴⁰¹ Indeed, the Baltimore City Police Department acknowledged using cell-site simulators to illegally spy on the city’s residents.⁴⁰²

In 2016, several organizations filed complaints with the Federal Communications Commission regarding the use of cell-site simulators by the Baltimore Police Department.⁴⁰³ To date, there is no decision by the FCC regarding this complaint.

CONCLUSION

The use of a cell-site simulator on the general population violates the Fourth Amendment regardless of whether analyzed pursuant to the trespass approach or based on a person’s reasonable expectation of privacy. In the trespass approach, the intrusion from the cell-site simulator travels from the device into a person’s home, car, clothing, etc. In other words, the simulator impacts all cell phones in protected areas. Pursuant to *Katz* and its progeny, a person has a reasonable expectation of privacy in a cell phone.

Across the country, we have seen law enforcement officers in Baltimore, Chicago, Miami, St. Louis, and more use cell-site simulators without warrants and in cases targeting protestors asserting their First Amendment rights. This targeting has focused on protest groups like Black Lives Matter and protests against police

399. Andrea Peterson, *FBI spy planes used thermal imaging tech in flights over Baltimore after Freddie Gray unrest*, WASH. POST (Oct. 30, 2015), <https://www.washingtonpost.com/news/the-switch/wp/2015/10/30/fbi-spy-planes-used-thermal-imaging-tech-in-flights-over-baltimore-after-freddie-gray-unrest/> (quoting an FBI spokesman as saying “FBI surveillance flights in support of the Baltimore Police Department in April were not collecting cellphone data, nor were they equipped with cell-site simulators”).

400. See Justin Fenton, *Baltimore Police Used Secret Technology to Track Cellphones in Thousands of Cases*, BALT. SUN (Apr. 9, 2015, 6:42 AM), <http://www.baltimoresun.com/news/maryland/baltimore-city/bs-md-citinggray-case-20150408-story.html> (“The Baltimore Police Department has used an invasive and controversial cellphone tracking device thousands of times in recent years while following instructions from the FBI to withhold information about it from prosecutors and judges . . .”).

401. Complaint For Relief Against Unauthorized Radio Operation And Willful Interference With Cellular Communications, *supra* note 146, at 7 (citation omitted).

402. David Walsh-Little, *No more secret surveillance on Baltimore citizens*, BALT. SUN (Aug. 24, 2016, 11:02 AM), <https://www.baltimoresun.com/opinion/op-ed/bs-ed-stingray-baltimore-20160824-story.html> (“Last year, [Baltimore Police Department] Detective Emmanuel Cabreja testified in a hearing in the Circuit Court for Baltimore City that this technology was used approximately 4,300 times during the past eight years — far from a small infringement on the privacy of Baltimore’s citizens.”).

403. See *id.*

killings of African-Americans.⁴⁰⁴ Indeed, as the GammaGroup brochure notes, its cell-site simulators typically can be operated for “[l]arge area coverage” in “particular areas of interest,” which is an ideal vague and cryptic way to describe spying on protests without specifically stating it.⁴⁰⁵ As Professor Nolan, a former police officer, explained, police can use this technology to engage in fishing expeditions in African-American communities: “Who’s to say police aren’t running Stingrays constantly in ‘hot spot’ areas? . . . Translation: communities of color The law-enforcement mentality is to get all the data and as much information as possible. . . .”⁴⁰⁶

Moreover, the Harris Corporation, the federal government, and local law enforcement agencies have created a cult of secrecy around the use of cell-site simulators.⁴⁰⁷ The FBI typically requires that police departments sign non-disclosure agreements in order to obtain this technology.⁴⁰⁸ This secrecy does not protect people whose cell phone data is inadvertently swept up in police surveillance.

There is little evidence as to whether cell-site simulators were used during the George Floyd protests since 2020.⁴⁰⁹ The United States Department of Justice approved authorization for the Drug Enforcement Agency to engage in covert surveillance around the country in response to the George Floyd protests.⁴¹⁰ Moreover, Attorney General William Barr issued a statement indicating federal agents with the FBI, the Marshals Service, the ATF, and the DEA will assist local law enforcement efforts regarding these protests.⁴¹¹ Protestors reported sudden cell

404. See Moy, *supra* note 398; see also Joseph, *supra* note 186 (discussing police use of cell-site simulators in Baltimore, Milwaukee, and Tallahassee noting that “police in these communities overwhelmingly use Stingrays in non-white and low-income communities”).

405. GAMMAGROUP, *3G-GSM Tactical Interception & Target Location*, at 8, <https://info.publicintelligence.net/Gamma-GSM.pdf> (last visited Sep. 26, 2021).

406. Joseph, *supra* note 186.

407. See Robert Patrick, *St. Louis police: We track cellphones, but won't tell you how*, ST. LOUIS POST-DISPATCH, (May 25, 2015), <https://bit.ly/3C21X5U>; Fred Clasen-Kelly, *Secrecy lifts in CMPD StingRay phone tracking*, CHARLOTTE OBSERVER (Feb. 15, 2015 10:15 PM); see also *Andrews v. Balt. City Police Dept.*, Civil No. CCB-16-2010, 2018 WL 3649602, at *2 n.3 (D. Md. Aug. 1, 2018) (unpublished); *In re United States for an Ord. Relating to Telephones Used by Suppressed*, No. 15 M 0021, 2015 WL 6871289, at *1 (N.D. Ill. Nov. 9, 2015) (discussing the non-disclosure agreement that Harris Corporation requires law enforcement using their devices to sign).

408. See Joseph, *supra* note 186.

409. See Cooper Quintin, *A Quick and Dirty Guide to Cell Phone Surveillance at Protests*, ELECTRONIC FRONTIER FOUNDATION (June 16, 2020), <https://www.eff.org/deeplinks/2020/06/quick-and-dirty-guide-cell-phone-surveillance-protests>.

410. See *Memorandum from Acting Adm'r Timothy Shea to Deputy Att'y Gen. Gerard Weinsheimer* (May 31, 2020), <https://www.documentcloud.org/documents/6935297-LEOPOLD-DEA-Memo-George-Floyd-Protests.html>; see also Lauren Frias, *The Justice Department reportedly granted DEA temporary power to conduct 'covert surveillance' on demonstrators at the George Floyd protests*, BUSINESS INSIDER (June 3, 2020, 1:13 AM), <https://www.businessinsider.com/doj-appoints-dea-surveillance-demonstrators-george-floyd-protests-report-2020-6> (discussing the Justice Department's authorization).

411. Press Release, Dept. of Justice, Attorney General William P. Barr's Statement on the Death of George Floyd and Riots (May 30, 2020), <https://www.justice.gov/opa/pr/attorney-general-william-p-barr-s-statement-death-george-floyd-and-riots>; see also Frias, *supra* note 411 (providing coverage of then-Attorney General Barr's statement).

phone coverage dead zones during protests, including near police stations.⁴¹²

In the end, although we do not know with one hundred percent certainty whether any police departments used cell-site simulators on protestors demonstrating against the death of George Floyd; given the cult of secrecy, the proliferation of such devices, and the use of them during protests by groups such as Black Lives Matter, it would be difficult to envision a scenario in which they were not used in such protests, in violation of the protestors Fourth Amendment rights. This trend of increased electronic surveillance is not only troubling but demonstrates a pattern of police conduct violative of the Fourth Amendment. More appellate courts and maybe someday the United States Supreme Court need to recognize that cell-site simulators violate the Fourth Amendment just as jurists for over a century have recognized that general warrants violate the Fourth Amendment.

412. Isaiah Holmes, *Milwaukee protestors and residents feel they're under police surveillance*, WIS. EXAM'R (June 23, 2020), <https://wisconsinexaminer.com/2020/06/23/milwaukee-protesters-and-residents-feel-theyre-under-police-surveillance/> (describing technological problems consistent with the impact of cell-site simulators usage).