Hastings Law Journal

Volume 66 | Issue 1 Article 4

12-2014

TriggerFish, StingRays, and Fourth Amendment Fishing Expeditions

Brian L. Owsley

TriggerFish, StingRays, and Fourth Amendment Fishing Expeditions

BRIAN L. OWSLEY*

Cell site simulators are an electronic surveillance device that mimics a cell tower causing all nearby cell phones to register their data and information with the cell site simulator. Law enforcement increasingly relies on these devices during the course of routine criminal investigations.

The use of cell site simulators raises several concerns. First, the federal government seeks judicial authorization to use such devices via a pen register application. This approach is problematic because a cell site simulator is different than a pen register. Moreover, the standard for issuance of a pen register is very low. Instead, this Article proposes that the applicable standard for granting a request to use a cell site simulator should be based on the Fourth Amendment probable cause standard.

Second, cell site simulators sweep up the data and information of innocent third-parties. The government fails to account for this problem. This Article proposes that the granting of an application for a cell site simulator should require a protocol for dealing with the third-party information that is captured.

---

* Brian L. Owsley, Assistant Professor of Law, Indiana Tech Law School; B.A., 1988, University of Notre Dame; J.D., 1993, Columbia University School of Law; M.I.A., 1994, Columbia University School of International and Public Affairs. From 2005 until 2013, the Author served as a United States Magistrate Judge for the U.S. District Court for the Southern District of Texas. I am very grateful for valuable comments and critiques provided by Steven Friedland, Jonah Horwitz, Stephen Wm. Smith, and Christopher Soghoian.

TABLE OF CONTENTS

INTRODUCTION

In recent years, traditional and online media have raised concerns about a means of electronic surveillance employed by the government that has various colorful and ominous names: TriggerFish, StingRay, AmberJack, KingFish, LoggerHead, Gossamer, Harpoon, Hailstorm, International Mobile Subscriber Identifier ("IMSI")[1] catcher, Electronic Serial Number ("ESN")[2] reader, cell site simulator, or digital analyzer.[3] The first eight names are essentially brand names of similar devices manufactured and sold by the Harris Corporation.[4] In the course of various criminal investigations, the government seeks to utilize an electronic device known as a StingRay that acts as a cell site simulator.[5] In other words, the device deceives nearby cell phones into believing that the device is a cell tower so that the cell phone's information is then downloaded into the cell site simulator.[6]

Imagine if you will, a federal agent sitting inside an unmarked van in a parking lot monitoring the activities of some subject of a criminal investigation. Inside the van the agent has an electronic surveillance device about the size of a bankers box connected to a laptop computer. With this device, the agent is targeting the subject's cell phone in a manner that the cell phone's number and other data, including,

---

1. *See In re* Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d), 964 F. Supp. 2d 674, 675 (S.D. Tex. 2013).

2. *See id.*

3. *See generally* Marc Rotenberg & David Brody, *Protecting Privacy: The Role of the Courts and Congress*, 39 HUM. RTS. 7 (2013); Jon Campbell, *LAPD Spied on 21 Using StingRay Anti-Terrorism Tool*, L.A. WEEKLY (Jan. 24, 2013), http://www.laweekly.com/2013-01-24/news/stingray-LAPD-spying-21-terrorism-tool-against-citizens; Ryan Gallagher, *FBI Files Unlock History Behind Clandestine Cellphone Tracking Tool*, SLATE (Feb. 15, 2013, 2:34 PM), www.slate.com/blogs/future_tense/2013/02/15/stingray_imsi_catcher_fbi_files_unlock_history_behind_cellphone_tracking.html; John Kelly, *It's Not Just the NSA: An Increasing Number of Police Agencies Across the USA Are Snatching Your Cellphone Data, Whether You're a Suspect or Not*, USA TODAY, Dec. 9, 2013, at A1; Leslie Meredith, *Law Enforcement Tracks Phones With Phony Cell Towers*, TECH NEWS DAILY (July 12, 2012), https://web.archive.org/web/20140531131028/http://www.technewsdaily.com/4537-embargoed-law-enforcement-tracks-real-phones-phony-cell-towers.html; Ellen Nakashima, *Little-Known Surveillance Tool Raises Questions Over Privacy*, WASH. POST, Mar. 28, 2013, at A3; Jennifer Valentino-Devries, *'Stingray' Phone Tracker Fuels Constitutional Clash*, WALL ST. J. (Sept. 22, 2011), http://online.wsj.com/article/SB10001424053111904194604576583112723197574.html; *see also* DAEHYUN STROBEL, IMSI CATCHER 1 (2007), *available at* http://www.emsec.rub.de/media/crypto/attachments/files/2011/04/imsi_catcher.pdf ("The IMSI Catcher is an expensive device to identify, track and tap a mobile phone user in such a way, that even the network operator cannot notice anything.").

4. HARRIS WIRELESS PRODS. GRP., HARRIS GCSD PRICE LIST, *available at* https://info.publicintelligence.net/Harris-SurveillancePriceList.pdf; Ryan Gallagher, *Meet the Machines That Steal Your Phone's Data*, ARS TECHNICA (Sept. 25, 2013, 10:00 AM), http://arstechnica.com/tech-policy/2013/09/meet-the-machines-that-steal-your-phones-data/.

5. *See* Nakashima, *supra* note 3; Campbell, *supra* note 3; Valentino-Devries, *supra* note 3.

6. *See* STROBEL, *supra* note 3, at 13–15.

potentially, voice communications, can be downloaded. This is a great device for apprehending the bad guys. Unfortunately, this device is capturing similar information from all the cell phones in the surrounding area. So the person who lives nearby, the couple who are sitting in the coffee shop on the corner, and you as you drive by in your car—all of you are also having your cell phone information captured and downloaded into the agent's computer. Let us assume that the agent obtained some kind of judicial authorization for this electronic surveillance. Would you want your information captured and saved in a government computer forever based only on the most minimal of standards? That is what the federal government is doing through its current use of cell site simulators.

Whatever these devices are called, they have proliferated in recent years, being used by state and federal law enforcement officials as well as by American and foreign intelligence agencies.[7] Not only are large law enforcement agencies like the Los Angeles Police Department using them,[8] but small cities like Gilbert, Arizona have also acquired them.[9] This technology, which has been patented since at least 2002,[10] has often been purchased with funds from the Department of Homeland Security to assist in regional terrorism investigations.[11] However, these devices have also come to be used for routine criminal investigations, including such offenses as burglary and murder.[12]

This Article addresses the use of cell site simulators and makes three principal points. First, the government's current approach of relying on the pen register statute to justify its requests for court orders fails because cell site simulators are not pen registers and thus are not

---

7. Kelly, *supra* note 3.

8. Campbell, *supra* note 3; *see* Cyrus Farivar, *Local Cops in 15 U.S. States Confirmed to Use Cell Tracking Devices*, ARS TECHNICA (June 12, 2014, 12:32 PM), http://arstechnica.com/tech-policy/2014/06/local-cops-in-15-us-states-confirmed-to-use-cell-tracking-devices.

9. In response to a request for information on electronic surveillance, Gilbert police officials informed the ACLU about their cell site simulator purchase: "The Gilbert Police Department obtained a $150,000 grant from the State Homeland Security Program. These funds, along with $94,195 of R.I.C.O. monies, were used to purchase cell phone tracking equipment in June 2008 (total acquisition cost of [$] 244,195)." Letter from Kate Weiby, Gilbert Police Legal Advisor, & Tim Dorn, Gilbert Chief of Police, to Dan Pochoda, ACLU (Sept. 6, 2011), *available at* http://www.aclu.org/files/assets/town_of_gilberts_response_to_prr_re_cell_phone_location_records.pdf; *accord* Bob Sullivan, *Pricey 'Stingray' Gadget Lets Cops Track Cellphones Without Telco Help*, NBC NEWS (Apr. 3, 2012, 2:47 AM), http://www.nbcnews.com/business/consumer/pricey-stingray-gadget-lets-cops-track-cellphones-without-telco-help-f635294. Based on the 2010 U.S. Census, Gilbert had an estimated population of 221,140 in 2012. *Gilbert Quick Facts*, U.S. CENSUS BUREAU, http://quickfacts.census.gov/qfd/states/04/0427400.html (last visited Dec. 14, 2014).

10. Allie Bohm, *You're Getting Warmer . . .*, ACLU BLOG OF RTS. (Sept. 26, 2011, 2:12 PM), http://www.aclu.org/blog/technology-and-liberty/youre-getting-warmer; *see* MMI Research Ltd. v. Cellxion Ltd., [2012] EWCA (Civ) 7 (Eng.).

11. Campbell, *supra* note 3; Joel Kurth & Lauren Abdel-Razzaq, *Oakland Deputies Use Cellphone Tracker—Military Device Sweeps All Calls Made in Wide Area*, DETROIT NEWS, Apr. 4, 2014, at A6.

12. Kurth & Abdel-Razzaq, *supra* note 11.

covered by the pen register statute. Second, the use of cell site simulators constitutes a Fourth Amendment search, which requires probable cause. Consequently, the proper approach is for the government to establish probable cause in order to obtain a search warrant consistent with the Fourth Amendment. Third, the use of the cell site simulators raises privacy concerns for third parties.

This Article raises the issue of cell site simulators in two ways that have not been addressed in current scholarship. First, I provide examples of court orders that address the use of these devices that have not been probed in previous legal scholarship. Second, I analyze the statutory and constitutional framework in which the government seeks to use cell site simulators. This Article provides a brief description of cellular telephone and cell site technology that concerns devices such as cell site simulators in Part I. Next, Part II provides a detailed description of how these types of devices operate. In Part III, the discussion documents the historical development of pen registers, including their statutory history. Part IV provides the various few examples of the government's applications for cell site simulators, as well as orders addressing such applications. Part V analyzes the development of Fourth Amendment jurisprudence and discusses the use of cell site simulators in light of people's reasonable expectations of privacy. In assessing these expectations, courts have, to a certain extent, relied on decisions that shape the third party doctrine—*Smith v. Maryland*[13] and *United States v. Miller*[14]—that no longer adequately address the realities of today's cell phone technology or people's expectations of privacy. Finally, in Part VI, I conclude by making some proposals as to how to address the privacy concerns.

I. CELL SITE SIMULATORS UTILIZE BASIC EXISTING CELLULAR TELEPHONE TECHNOLOGY

To fully appreciate the significance of a cell site simulator, it is important to understand the basics of how cellular telephones work. In enacting the Electronic Communications Privacy Act ("ECPA"), Congress addressed cellular telephones, which at that time were based on radio transmission.[15] In building a network, telecommunications

13. 442 U.S. 735 (1979).

14. 425 U.S. 435 (1976).

15. *See* Timothy B. Lee, *Documents Show Cops Making Up the Rules on Mobile Surveillance*, ARS TECHNICA (Apr. 3, 2012, 7:40 AM) http://arstechnica.com/tech-policy/2012/04/documents-show-cops-making-up-the-rules-on-mobile-surveillance; *see also In re* Application of the U.S. 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* Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 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."); Brian Owsley, *The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in its Electronic Surveillance*, 16 U. PA. J. CONST. L. 1, 3 (2013).

providers created "large service areas [that] are divided into honeycomb-shaped segments or 'cells'—each of which is equipped with a low-power transmitter or base station which can receive and radiate messages within its parameters" from cellular phones within the providers' networks.[16] Each "cell," in turn, collects "a number of pieces of data 'regarding the strength, angle, and timing of the caller's signal measured at two or more cell sites, as well as other system information such as a listing of all cell towers in the market area, switching technology, protocols, and network architecture.'"[17] Consequently, each cell site "detects the radio signal from the handset, and connects it to the local telephone network, the Internet, or another wireless network."[18] Typically, cell sites are physically located atop towers, but the equipment can also be placed on trees, roofs, flagpoles, and buildings.[19]

Within this framework of cell tower networks, the origination of a cellular telephone call initiates a series of relays along the cell site network:

> When a caller dials a number on a cellular telephone, a transceiver sends signals over the air on a radio frequency to a cell site. From there the signal travels over phone lines or a microwave to a computerized mobile telephone switching office ("MTSO") or station. The MTSO automatically and inaudibly switches the conversation from one base station and one frequency to another as the portable telephone . . . moves from cell to cell.[20]

Whenever any cellular phone is turned on, it sends out a signal seeking the closest cell site, which in turn will register that telephone with that

---

16. S. REP. NO. 99-541, at 9 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3563; *see* In re *Application for Pen Register & Trap/Trace Device*, 396 F. Supp. 2d 750 ("'Cell' refers to geographic regions often illustrated as hexagons, resembling a bee's honeycomb; a 'cell site' is where the radio transceiver and base station controller are located (at the point three hexagons meet)."); Aaron Blank, *The Limitations and Admissibility of Using Historical Cellular Site Data to Track the Location of a Cellular Phone*, 18 RICH. J.L. & TECH. 3, 4 (2011) (discussing the honeycomb pattern creating cells); 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 (2012) ("Service providers maintain large numbers of radio base stations (also called 'cell sites') spread through their geographic coverage areas. These cell sites are generally located on 'cell towers' serving geographic areas of varying sizes, depending upon topography and population concentration.").

17. Ian Herbert, *Where We Are with Location Tracking: A Look at the Current Technology and the Implications on Fourth Amendment Jurisprudence*, 16 BERKELEY J. CRIM. L. 442, 478 (2012) (quoting *In re Application for Pen Register & Trap/Trace Device*, 396 F. Supp. 2d at 749); *see* Owsley, *supra* note 15, at 3–4.

18. *In re Application of the U.S. for Historical Cell Site Data*, 747 F. Supp. 2d at 831 (citations omitted).

19. *Id.*; *see* Owsley, *supra* note 15, at 4.

20. S. REP. NO. 99-541, at 9; *see* Pell & Soghoian, *supra* note 16, at 127 ("mobile 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"); Owsley, *supra* note 15, at 4.

cell site.[21] "This process, called 'registration,' occurs approximately every seven seconds,"[22] enabling "cellular providers to obtain a plethora of information about the telephones contacting their cell-sites."[23]

The Department of Justice ("DOJ") has explained that "to provide service to cellular telephones, providers have the technical capability to collect information such as the cell tower nearest to a particular cell phone, the portion of that tower facing the phone, and often the signal strength of the phone."[24] For example, in 1997, the Federal Communications Commission ("FCC") issued rules "requir[ing] cellular service providers to upgrade their systems to identify more precisely the longitude and latitude of mobile units making emergency 911 calls."[25] Telecommunications providers "generally keep detailed historical records of this information for billing and other business purposes."[26]

This network of cell towers was designed to further communication among a subscriber's cell phone with other cell phones or landline telephones. It is necessary for efficient operation of the network. It is unlikely to change in any significant manner because the complete

---

21. *ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the Comm. on the Judiciary*, 111th Cong. 13–14 (2010) (statement of Matt Blaze, Associate Professor, University of Pennsylvania); Stephanie K. Pell & Christopher Soghoian, *A Lot More than a Pen Register, and Less than a Wiretap*, 16 YALE J. L. & TECH. 134, 144 (2014); Blank, *supra* note 16, at 5; *see* Owsley, *supra* note 15, at 5.

22. *In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 534 F. Supp. 2d 585, 590 (W.D. Pa. 2008) (citation omitted), *rev'd on other grounds*, 620 F.3d 304, 313 (3d Cir. 2010); *accord* Owsley, *supra* note 15, at 5; Kevin McLaughlin, Note, *The Fourth Amendment and Cell Phone Location Tracking: Where Are We?*, 29 HASTINGS COMM. & ENT. L.J. 421, 426 (2007).

23. Owsley, *supra* note 15, at 5.

24. U.S. DEP'T OF JUSTICE, ELECTRONIC SURVEILLANCE MANUAL 41 (rev. 2005) [hereinafter ELECTRONIC SURVEILLANCE MANUAL], *available at* www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf; *see In re* Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 115 (E.D.N.Y. 2011) ("Cell phones work by communicating with cell-sites operated by cell-phone service providers. Each cell-site operates at a certain location and covers a certain range of distance.").

25. *In re* Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 532 (D. Md. 2011); *see* Laurie Thomas Lee, *Can Police Track Your Wireless? Call Location Information and Privacy Law*, 21 CARDOZO ARTS. & ENT. L.J. 381, 384–86 (2003) (discussing the FCC's enhanced 9-1-1 regulations); 47 C.F.R. § 20.18(h) (2013) (setting accuracy standards for cell phone calls within targeted distances).

26. ELECTRONIC SURVEILLANCE MANUAL, *supra* note 24, at 41; *In re* Application of the U.S. for & Order: (1) Authorizing the Use of a Pen Register & Trap & Trace Device; (2) Authorizing Release of Subscriber & Other Info.; & (3) Authorizing the Disclosure of Location-Based Servs., 727 F. Supp. 2d 571, 573 (W.D. Tex. 2010) (cell site location information "is information that resides on computer servers of telecommunications providers"); *see In re* Application of the U.S. for an Order Authorizing the Use of a Cellular Tel. Digital Analyzer, 885 F. Supp. 197, 199 (C.D. Cal. 1995) ("The telephone company uses this information both to bill the subscriber of the cellular telephone based on its usage and also to connect the cellular telephone to the telephone number called."); Pell & Soghoian, *supra* note 16, at 128 ("Wireless service providers retain detailed logs for diagnostic, billing, and other purposes.").

overhaul of the technology would be expensive. It is this system of cell tower networks that government officials seek to utilize when employing cell site simulators.

Most cellular telephones around the world operate through the Global System for Mobile Communications ("GSM").[27] Within this system, a cell phone initiating a call connects through its unique International Module Equipment Identity ("IMEI")[28] to a base station, which is essentially the hardware of a cell tower.[29] A base station potentially can operate with signal strength as low as fifty watts.[30] Of course, the number of base stations in an area hinges on the volume of demand for cellular service in that area:

> The size of the cell depends basically on the geographic features of the area and consequently on the range of the stations. But also the number of possible calls, that have to be handled simultaneously, has to be considered, since it is limited by the number of available channels. Hence, in densely populated areas, the cells often have a diameter of only a few hundred meters, whereas in sparsely populated areas several kilometers are usual.[31]

A base station is "not only responsible for the connectivity [of the cell phone call, but is] also needed for encryption and decryption of communication data."[32] From the base station, a cell phone call is routed to a base station controller, which in turn will move the call to another base station to prevent the call from being terminated.[33] If this handoff has to be done beyond a base station controller's range, then the transfer is handled by a mobile switching center.[34] This transfer represents the final stage of the call as the mobile switching center "is responsible for the authentication, routing, handoffs over different Base Station Controllers, connection to the landline, etc."[35]

---

27. STROBEL, *supra* note 3, at 3 ("GSM is the most common standard for communication. It is used in more than 200 countries and territories all over the world."); Karsten Nohl & Chris Paget, *GSM—SRSLY?*, CHAOS COMMC'N CONG. 2 (Dec. 27, 2009), http://events.ccc.de/congress/2009/Fahrplan/attachments/1519_26C3.Karsten.Nohl.GSM.pdf (noting that GSM is used by eighty percent of the cell phone market, with over four billion users).

28. *In re* Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d), 964 F. Supp. 2d 674, 675 (S.D. Tex. 2013); *see Analysis of IMEI Numbers*, INT'L NUMBERING PLANS, https://www.numberingplans.com/?page=analysis&sub=imeinr (last visited Dec. 14, 2014) ("All mobile phones are assigned a unique 15 digit IMEI code upon production.").

29. *See* STROBEL, *supra* note 3, at 4; *see also GSM—The Base Station Subsystem (BSS)*, TUTORIALSPOINT, http://www.tutorialspoint.com/gsm/gsm_base_station_subsystem.htm (last visited Dec. 14, 2014).

30. STROBEL, *supra* note 3, at 13; David Talbot, *A 50-Watt Cellular Network*, MIT TECH. REV. (Feb. 10, 2010), http://www.technologyreview.com/news/417442/a-50-watt-cellular-network.

31. STROBEL, *supra* note 3, at 4.

32. *Id.*

33. *Id.* at 4–5; *see* Blank, *supra* note 16, at 5–6 (discussing the handoff process).

34. STROBEL, *supra* note 3, at 5.

35. *Id.*

II. Cell Site Simulators Capitalize on Existing Cellular Technology to Retrieve a Cell Phone User's Information

Understanding how cell phone technology works, it is next important to appreciate how cell site simulators exploit cell phone technology in order to gather electronic information.

A. Basic Operations of Cell Site Simulators

Cell site simulators are being used more and more by intelligence agencies around the world, not just in the United States.[36] Although the Harris Corporation is one of the major producers of these devices, these days, a reasonably bright computer whiz with $1,500 can buy the raw components to make one.[37] The names TriggerFish and StingRay are trade names manufactured by the Harris Corporation, which sells those devices to American law enforcement and intelligence agencies.[38] Essentially, a TriggerFish is an older piece of technology that is a digital analyzer for passive interception of analog cell phone service.[39] In other words, while it can intercept a cell phone call's verbal content, a digital analyzer (because it is a passive surveillance technique) can intercept only cell phones that are actually transmitting.

On the other hand, a StingRay is an IMSI catcher that captures digital cell phone information through an active interception process.[40] In 1996, Rohde & Schwarz, a German electronics company specializing in wireless communications, first invented an IMSI catcher that was able "to identify a subscriber by forcing it to transmit the IMSI."[41] One year later, the next model created by Rohde & Schwarz enabled the user "not

---

36. *See* Ryan Gallagher, *Criminals May Be Using Covert Mobile Phone Surveillance Tech for Extortion*, Slate (Aug. 22, 2012, 9:00 AM), http://www.slate.com/blogs/future_tense/2012/08/22/imsi_catchers_criminals_law_enforcement_using_high_tech_portable_devices_to_intercept_communications_.html.

37. Chris Soghoian, Cellular Phones and Mobile Privacy: Direct Government Surveillance (Stingrays), Location Tracking and Biometrics Conference at Yale Law School (Mar. 3, 2013), *available at* http://www.youtube.com/watch?v=OwutGSjNQok.

38. Declan McCullagh, *FBI Prepares to Defend 'Stingray' Cell Phone Tracking*, CNET (Mar. 27, 2013, 4:57 PM), http://news.cnet.com/8301-13578_3-57576690-38/fbi-prepares-to-defend-stingray-cell-phone-tracking; Valentino-Devries, *supra* note 3. Interestingly, while the Harris Corporation notes a number of the products and services it provides to customers on its websites, it does not address this electronic surveillance technology. Harris, http://www.harris.com (last visited Dec. 14, 2014).

39. Location Tracking and Biometrics Conference, *supra* note 37; *see* Gallagher, *supra* note 4; *see also In re* Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 755 (S.D. Tex. 2005) (defining a TriggerFish as a device that "enables law enforcement to gather cell site data directly, without the assistance of the service provider").

40. Location Tracking and Biometrics Conference, *supra* note 37; Nohl & Paget, *supra* note 27.

41. Strobel, *supra* note 3, at 13; *see* MMI Research Ltd. v. Cellxion Ltd., [2012] EWCA (Civ) 7, [4] (Eng.) ("These are devices used by the police and security services to discover the mobile phone numbers of suspected criminals or terrorists. Every mobile phone has an 'IMSI' associated with its SIM card, which is its permanent identity number.").

only to identify, but also to tap outgoing calls."[42] Thus, as early as 1997, an IMSI catcher could be used to capture audio content.

Within the GSM, there is a vulnerability in the authentication process that enables cell site simulators, like an IMSI catcher, to breach the system.[43] Specifically, "it is not necessary to authenticate a Base Station to a Mobile Station."[44] In other words, the cell site simulator tricks the nearby cell phone into transmitting information to it as it would the nearest cell tower. "An IMSI catcher exploits this weakness and masquerades to a Mobile Station as a Base Station."[45] Through this masquerade, the cell site simulator "causes every mobile phone of the simulated network operator within a defined radius to log in" or register with it as it would a cell tower.[46]

Cell phones are designed to optimize reception by seeking the strongest signal among nearby base stations.[47] A base station can operate effectively with signal strength as low as twenty-five watts.[48] Thus, for a cell site simulator to be effective, it need only be marginally stronger than the signal of the nearest cell towers.

B. The Manner in Which Law Enforcement Officials Use Cell Site Simulators

Law enforcement officials will often use a cell site simulator inside a vehicle in conjunction with a computer that has mapping software.[49] Normally when a cellular phone is turned on, it seeks a connection to its telecommunications network system by using the nearest cell tower within its network.[50] This registration process enables the cell phone to communicate with its network, transmitting information and data, including audio content. Capitalizing on this registration, after the cell

---

42. Strobel, *supra* note 3, at 13; *see Integrated Ratio Communication Network—Rohde & Schwarz*, Tiara Commc'ns, https://web.archive.org/web/20090209050710/http://tiaracom.com.my/rohde&schwarz.htm (last visited Dec. 14, 2014) (informational sheet from Rohde & Schwarz regarding its IMSI catcher's capacities).

43. Strobel, *supra* note 3, at 7.

44. *Id.* at 13.

45. *Id.*; Pell & Soghoian, *supra* note 21, at 145–46; *see MMI Research*, [2012] EWCA (Civ) 7, [5] (Noting the IMSI catcher created by Rohde & Schwarz "involves the creation of a false base station. Mobile phones in a particular area will transmit information to a base station which operates as a transmitter and a receiver to and from the phones. The IMSI catcher uses a false base station which is constructed in a manner which leads the phone to believe it is genuine, and thereby to communicate with it.").

46. Strobel, *supra* note 3, at 13; Kelly, *supra* note 3; Pell & Soghoian, *supra* note 21, at 147–48.

47. Strobel, *supra* note 3, at 13; Blank, *supra* note 16, at 5 ("When a user places a call, the cell phone connects to the cell site with the strongest signal.").

48. Strobel, *supra* note 3, at 13.

49. Kelly, *supra* note 3; Jennifer Valentino-Devries, *How 'Stingray' Devices Work*, Wall St. J. (Sept. 21, 2011, 10:33 PM), http://blogs.wsj.com/digits/2011/09/21/how-stingray-devices-work.

50. Kelly, *supra* note 3; Jon Campbell, *LAPD Spy Device Taps Your Cell Phone*, L.A. Weekly (Sept. 13, 2012), http://www.laweekly.com/2012-09-13/news/LAPD-stingray-spying-cellphone.

site simulator mimics a cell tower, nearby cellular phones will connect to it. This connection enables the device to download telephone numbers and other information related to the cellular phones, such as signal strength, because it typically emits the strongest signal in the nearby area.[51] For example, this technology would enable the user of a cell site simulator to detect the electronic serial number of the phone, the number for the cellular telephone, as well as any telephone numbers called from the cell phone.[52] The surveillance vehicle can then move to several different locations, collecting the phone's signal strength, thus enabling the officers to triangulate and map the phone's location.[53]

In addition to downloading information from all the cellular phones located within the area, a cell site simulator can be used to locate a specific cellular phone when the number is already known, but the location is unknown.[54] Law enforcement officials "can drive around until they get a signal from the target phone while pinging it."[55] After the target phone is located, the signal strength is measured in order to triangulate and map the location again.[56] In a hearing addressing electronic surveillance issues, an FBI agent "testified that he was able to determine the approximate distance from the originating cell tower where the cell phone and Stingray switched from the originating cell tower to another cell tower."[57] He further explained "that this method allows him to determine, with a reasonable degree of certainty, a fairly narrow geographical location where an individual is located while a cell call is being placed."[58]

Similarly, in a warrantless search by the Tallahassee Police Department, officers used a handheld device, as well as one mounted on

---

51. Valentino-Devries, *supra* note 49; Campbell, *supra* note 50.

52. *In re* Application of the U.S. for an Order Authorizing the Use of a Cellular Tel. Digital Analyzer, 885 F. Supp. 197, 199 (C.D. Cal. 1995).

53. Valentino-Devries, *supra* note 49; *see* Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 712–13 (2011) (discussing triangulation).

54. Valentino-Devries, *supra* note 49.

55. *Id.* Pinging is the system by which a cell phone sends out data to register with the nearest cell phone towers. *Id. See* United States v. Allums, No. 2:08-CR-30 TS, 2009 WL 806748, at *3 (D. Utah Mar. 24, 2009) (discussing an agent driving around with the device); United States v. Rigmaiden (*Rigmaiden I*), 844 F. Supp. 2d 982, 995 (D. Ariz. 2012) ("The FBI used the device in multiple locations. The FBI analyzed signals exchanged between the mobile tracking device and the aircard. The FBI would take a reading, move to another location, take another reading, move to another location, etc."); United States v. Rigmaiden (*Rigmaiden II*), No. CR 08-814-PHX-DGC, 2013 WL 1932800, at *15 (D. Ariz. May 8, 2013) (same).

56. Valentino-Devries, *supra* note 49.

57. *Allums*, 2009 WL 806748, at *1; *see* Blank, *supra* note 16, at 30–31 (discussing the admissibility of expert testimony by the FBI agent).

58. *Allums*, 2009 WL 806748, at *1.

a police vehicle.[59] Testimony from an unsealed hearing transcript revealed how the cell site simulators were employed:

> Police drove through the area using the vehicle-based device until they found the apartment complex in which the target phone was located, and then they walked around with the handheld device and stood 'at every door and every window in that complex' until they figured out which apartment the phone was located in. In other words, police were lurking outside people's windows and sending powerful electronic signals into their private homes in order to collect information from within.[60]

Consistent with the testimony in *United States v. Allums*, it is apparent that some law enforcement officials are personally using this technology, as opposed to relying on any third-party telecommunications providers.

Any signals sent by law enforcement officials using a cell site simulator are signals that would not otherwise have been sent during the normal operations of a telecommunication provider's operation of its cell towers.[61] Moreover, the use of this device causes a brief disruption in the telecommunication provider's service to the cell phone.[62]

Some law enforcement officials are utilizing cell site simulators without court authorization.[63] Moreover, the federal officials who do seek a court order routinely file such applications pursuant to the pen register statute.[64] This approach is highly advantageous for the government, as the standard for a pen register application is much lower than the standard for a warrant because it does not require probable cause.[65]

III. The Development of the Pen Register Statute

In order to analyze the inapplicability of the pen register statute to cell site simulators, one must know the function of a pen register. When the government seeks to ascertain the telephone numbers of incoming

---

59. *See* Thomas v. State, 127 So. 3d 658, 660 (Fla. Dist. Ct. App. 2013); Nathan Freed Wessler, *Victory: Judge Releases Information About Police Use of Stingray Cell Phone Trackers*, ACLU (June 3, 2014, 3:12 PM), https://www.aclu.org/blog/national-security-technology-and-liberty/victory-judge-releases-information-about-police-use.

60. *See* Wessler, *supra* note 59.

61. *Rigmaiden I*, 844 F. Supp. 2d 982, 995 (D. Ariz. 2012); *Rigmaiden II*, No. CR 08-814-PHX-DGC, 2013 WL 1932800, at *15 (D. Ariz. May 8, 2013).

62. *Rigmaiden I*, 844 F. Supp. 2d at 995; *Rigmaiden II*, 2013 WL 1932800, at *15.

63. *See* Wessler, *supra* note 59 (noting that Tallahassee police were using a StingRay without a warrant).

64. 18 U.S.C. § 3123 (2012).

65. *Compare id.* § 3123(a)(1) (a pen register order is issued "if the court finds that the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation"), *with* Fed. R. Crim. P. 41(d)(1) ("After receiving an affidavit or other information, a magistrate judge—or if authorized by Rule 41(b), a judge of a state court of record—must issue the warrant if there is probable cause to search for and seize a person or property or to install and use a tracking device.").

and outgoing calls, it files an application seeking a court order authorizing a pen register and a trap and trace device, respectively.[66] Historically, the Supreme Court defined a pen register as a device recording the outgoing numbers dialed from a specific telephone.[67] In *United States v. New York Telephone Company*,[68] the Court similarly defined a pen register: "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."[69] In other words, the Court reiterated the position from *United States v. Giordano*, that a pen register concerns the telephone numbers of outgoing calls from a specific telephone.

In *New York Telephone*, the Supreme Court held that Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Wiretap Act") did not apply to pen registers.[70] Instead, the Court held that the statute concerned only "orders 'authorizing or approving the *interception* of a wire or oral communication.'"[71] Because pen registers do not intercept any communications, the Wiretap Act did not authorize pen registers. Nonetheless, the Court concluded that district courts have the authority to authorize the installation of a pen register.[72] The basis for this authority was Rule 41 of the Federal Rules of Criminal Procedure, which requires a showing of probable cause.[73] Specifically, the Court reasoned "that Rule 41 is sufficiently broad to include seizures of intangible items such as dial impulses recorded by pen registers."[74]

---

66. *See generally* ELECTRONIC SURVEILLANCE MANUAL, *supra* note 24, at 38–40.

67. *See* United States v. Giordano, 416 U.S. 505, 511 n.2 (1974) (noting that a pen register is "a device that records telephone numbers dialed from a *particular phone*") (emphasis added); *see also id.* at 549 n.1 (Powell, J., concurring in part and dissenting in part) ("A pen register is a mechanical device attached to a given telephone line and usually installed at a central telephone facility. It records on a paper tape all numbers dialed from that line. It does not identify the telephone numbers from which incoming calls originated, nor does it reveal whether any call, either incoming or outgoing, was completed. Its use does not involve any monitoring of telephone conversations.").

68. 434 U.S. 159 (1977).

69. *Id.* at 161 n.1; *see* 18 U.S.C. § 3127(3) (2012).

70. 434 U.S. at 166; *see* David McPhie, *Almost Private: Pen Registers, Packet Sniffers, and Privacy at the Margin*, 2005 STAN. TECH. L. REV. 1, 8 ("Almost ten years after Title III had been signed into law, the Supreme Court in *United States v. New York Telephone Company* relied on th[e] legislative history and the statutory language in holding that pen registers did not intercept the 'contents' of communications, and so did not fall within the scope of Title III.").

71. *N.Y. Tel.*, 434 U.S. at 166 (quoting 18 U.S.C. § 2518(1) (1976)) (emphasis in original).

72. *Id.* at 168.

73. *Id.* at 168–69; *see* FED. R. CRIM. P. 41(d) ("After receiving an affidavit or other information, a magistrate judge . . . must issue the warrant if there is probable cause to search for and seize a person or property or to install and use a tracking device.").

74. *N.Y. Tel.*, 434 U.S. at 170.

In 1986, Congress enacted the ECPA, which amended the Wiretap Act to explicitly address pen registers.[75] The ECPA defined a pen register as a "device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted . . . on the telephone line to which such device is attached."[76] This definition essentially follows the definition enunciated in *New York Telephone*.

In the Communications Assistance for Law Enforcement Act of 1994, Congress mandated that both telecommunications and Internet service providers permit authorized law enforcement officers access to their networks in order for them to engage in electronic surveillance.[77] Regarding pen registers, however, the statute required that use of such technology "shall not include any information that may disclose the physical location of the subscriber."[78] Through this revision, Congress sought to capture transmitted e-mail data as well as the outgoing number dialed on cell phones, but not the location of the cell phone itself. In testifying before Congress in support of the statute, then-FBI Director Louis Freeh attempted to assuage legislators' concerns the statute would be used to authorize the tracking of individuals.[79]

In 2001, Congress amended the definition of the term "pen register" in the USA Patriot Act.[80] The Patriot Act defines a "pen register" as "a device or process which records or decodes dialing, routing, addressing,

---

75. S. REP. No. 99-541, at 9 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3557 ("Title III of the bill addresses pen registers.").

76. Electronics Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.); *In re* Application of the U.S. for an Order Authorizing the Use of a Cellular Tel. Digital Analyzer, 885 F. Supp. 197, 200 (C.D. Cal. 1995) (addressing the statutory definition); *accord* United States v. Forrester, 512 F.3d 500, 512 (9th Cir. 2008) (citing 18 U.S.C. § 3127(3) and explaining this pen register definition applied when the surveillance occurred, between May and July 2001); Donahue v. Gavin, 280 F.3d 371, 373 n.3 (3d Cir. 2002); Brown v. Waddell, 50 F.3d 285, 290 (4th Cir. 1995) (citing 18 U.S.C. § 3127(3)); *see* U.S. Telecom Ass'n v. FCC, 227 F.3d 450, 454 (D.C. Cir. 2000) ("Pen registers record telephone numbers of outgoing calls.").

77. *See generally* Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified as amended in scattered sections of 47 U.S.C.); *see also* Timothy Casey, *Electronic Surveillance and the Right to Be Secure*, 41 U.C. DAVIS L. REV. 977, 1003 (2008).

78. 47 U.S.C. § 1002(a)(2)(B) (2011).

79. *See Police Access to Advanced Communication Systems: Hearing Before the Subcomm. on Tech. & the Law of the Comm. on the Judiciary, U.S. S., and the Subcomm. on Civil & Constitutional Rights of the Comm. on the Judiciary, H.R.*, 103d Cong. (1994) (statement of Louis J. Freeh, Director, FBI), *available at* 1994 WL 223962; *see also In re* Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register, 415 F. Supp. 2d 211, 216–17 (W.D.N.Y. 2006) (discussing Director Freeh's testimony); *In re* Application of the U.S. for an Order Authorizing the Disclosure of Prospective Cell Site Info., 412 F. Supp. 2d 947, 955 (E.D. Wis. 2006) (same).

80. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified as amended in scattered sections of 8, 12, 15, 18, 20, 31, 42, 47, 49, 50 and 51 U.S.C.); *see In re* Application of the U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., 460 F. Supp. 2d 448, 455 (S.D.N.Y. 2006) (discussing legislative history).

or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication."[81] An order authorizing a pen register pursuant to the Patriot Act must specify:

> (A) the identity, *if known*, of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied;
>
> (B) the identity, *if known*, of the person who is the subject of the criminal investigation;
>
> (C) the attributes of the communications to which the order applies, including the number or other identifier and, *if known*, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied.[82]

Analysis of § 3123(b)(1) reveals that, in each subsection, Congress inserted the language "if known" to specify that the order need only contain the aforementioned information if known at the time authorization is requested. For example, in subsection (A), the order need not contain the name of the person to whom the cell phone is leased unless that person's name is known. Similarly, in subsection (B), the court order does not have to provide the name of the target of the investigation unless that person's name is known. However, in subsection (C), Congress did not modify the language "the attributes of the communications to which the order applies, including the number or other identifier" to add "if known." Indeed, the word "and" in that subsection makes clear that "the location of the telephone line or other facility" must be included in the order only "if known." Consequently, the rest of "the attributes of communications," including "the number or other identifier," must be specified within any order authorizing any pen register application.

Moreover, the inclusion of the word "facility" within the text of § 3123(b)(1), in addition to "telephone line," as covered by the pen register statute, does not permit law enforcement to obtain subscriber information without providing the cell phone number. The DOJ

---

81. 18 U.S.C. § 3127(3) (2012); *see* United States v. Jadlowe, 628 F.3d 1, 6 n.4 (1st Cir. 2010) ("A 'pen register' is a device used, inter alia, to record the dialing and other information transmitted by a targeted phone."). The Patriot Act distinguished a pen register from a trap and trace device, which is defined as "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication." 18 U.S.C. § 3127(4).

82. 18 U.S.C. § 3123(b)(1) (2012) (emphasis added); *see* Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1431–32 (2004) ("[T]he statute required the court order to specify the number of the 'telephone line' to which the pen register or trap and trace would be attached.").

acknowledged that "facility" would include "a cellular telephone number" or "a specific cellular telephone identified by its electronic serial number."[83] Pursuant to § 3123(b)(1), pen register applicants can make requests when they know the cell phone number or the electronic serial number.[84] Indeed, the DOJ's *Field Guidance on New Authorities that Relate to Computer Crime and Electronic Evidence*s suggests that a pen register is not appropriate when the targeted cell phone number or electronic serial number is unknown. Much of the significance of the amending language is attributable to the fact that Congress sought to ensure that the use of pen registers extended to new technologies, such as cell phones and computers.[85]

Accordingly, this revision in the USA Patriot Act broadened the definition of a pen register. Some judges have interpreted the Patriot Act to expand the definition to include electronic communications in addition to dialing information, but not to the capture of cell site information.[86] Others have rejected this approach, concluding that the Patriot Act applies to all communications to and from the targeted cell phone.[87] Regardless of the debate over the scope of a pen register following the Patriot Act, courts have routinely determined that law enforcement submit an application to use a pen register when seeking information about a particular telephone.[88] Indeed, the purpose of a pen register is to track telephone numbers, not people.

---

83. U.S. DEP'T OF JUSTICE, COMPUTER CRIME AND INTELLECTUAL PROP. SECTION, FIELD GUIDANCE ON NEW AUTHORITIES THAT RELATE TO COMPUTER CRIME AND ELECTRONIC EVIDENCE ENACTED IN THE USA PATRIOT ACT OF 2001 4 (2001), *available at* https://www.student.cs.uwaterloo.ca/~cs492/papers/ccips.pdf [hereinafter FIELD GUIDANCE ON NEW AUTHORITIES]; *see* Patricia Mell, *Big Brother at the Door: Balancing National Security with Privacy Under the USA Patriot Act*, 80 DENV. U. L. REV. 375, 402 n.226 (2002).

84. FIELD GUIDANCE ON NEW AUTHORITIES, *supra* note 83, at 4.

85. *See id.* at 5.

86. *In re* Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 753 n.8 (S.D. Tex. 2005); *accord In re* Application of the U.S. for an Order (1) Authorizing the Use of Pen Register & a Trap & Trace Device & (2) Authorizing Release of Subscriber Information and/or Cell Site Information, 396 F. Supp. 2d 294, 318 (E.D.N.Y. 2005) (adopting the reasoning of *In re Application for Pen Register & Trap/Trace Device*, 396 F. Supp. 2d 747).

87. *In re* Application of the U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., 460 F. Supp. 2d 448, 456 (S.D.N.Y. 2006); *see In re* Application of the U.S. for an Order Authorizing the Use of a Pen Register & Trap on [xxx]Internet Service Account/User Name [xxxxxxxxxx@xxx.com], 396 F. Supp. 2d 45, 49–50 (D. Mass. 2005) ("There can be no doubt that the expanded definition of a pen register, especially the use of the term 'device or *process*,' encompasses e-mail communications and communications over the internet.") (emphasis in original).

88. United States v. Jadlowe, 628 F.3d 1, 6 n.4 (1st Cir. 2010); *In re* Applications of the U.S. for Orders (1) Authorizing the Use of Pen Registers & Trap & Trace Devices & (2) Authorizing Release of Subscriber Info., 515 F. Supp. 2d 325, 328 (E.D.N.Y. 2007) ("In layman's terms, a pen register is a device capable of recording all digits dialed from a particular telephone."); United States v. Bermudez, No. IP 05-43-CR-B/F, 2006 WL 3197181, at *8 (S.D. Ind. June 30, 2006) (unpublished) ("A 'pen register' records telephone numbers dialed for outgoing calls made from the target phone."); *In re Application of the U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular*

In *New York Telephone*, the Supreme Court's conclusion that the Wiretap Act did not apply to pen registers did not also mean that the government could obtain pen registers without any judicial intervention.[89] To the contrary, the Court determined that the government could only obtain a pen register by establishing probable cause, consistent with the seizure standard enunciated in Rule 41 of the Federal Rules of Criminal Procedure, which is based on the Fourth Amendment.[90] Even if cell site simulators are not covered by the current iteration of the pen register statute, that does not grant the government carte blanche to use these devices without any judicial authorization. Instead, the appropriate approach is for the government to seek authorization for the use of a cell site simulator consistent with the requirements of Rule 41 and the Fourth Amendment.

Congress has limited judicial review of pen register applications to the "ministerial" task of confirming that the government has properly identified the attorney and agency seeking the order as well as providing a certification that the information sought through the device is relevant to an ongoing investigation.[91] When reviewing these applications, courts inquire neither into the veracity of the facts asserted by the government, nor into the reasonableness of its judgment concerning likelihood or relevance.[92] One scholar notes that "the ECPA's vague definition of a pen register, in combination with innovations in communications technologies and judicial permissiveness, allows law enforcement to acquire much communication attribute information by satisfying, at most, the minimal pen register procedures."[93] Consequently, the government is typically able to provide the proper identifications and

---

Tel., 460 F. Supp. 2d at 455 (pen registers apply to particular cell phones); *In re* Application of the U.S. for an Order for Disclosure of Telecomm. Records & Authorizing the Use of a Pen Register & Trap & Trace, 405 F. Supp. 2d 435, 438 (S.D.N.Y. 2005) ("Pen Register Statute is the statute used to obtain information on an ongoing or prospective basis regarding outgoing calls from a particular telephone."); *In re* Application of U.S. for an Order Authorizing Installation & Use of a Pen Register & a Caller Identification Sys. on Tel. Nos. [Sealed] & [Sealed] & the Production of Real Time Cell Site Info., 402 F. Supp. 2d 597, 602 (D. Md. 2005) ("A pen register records telephone numbers dialed for outgoing calls from the target phone . . ."); *In re Application for Pen Register & Trap/Trace Device*, 396 F. Supp. 2d at 752 ("A 'pen register' is a device that records the numbers dialed for outgoing calls made from the target phone.").

89. *See* United States v. N.Y. Tel. Co., 434 U.S. 159, 170 (1977).

90. *See id.*

91. 18 U.S.C. § 3122 (2012); *see* United States v. Fregoso, 60 F.3d 1314, 1320 (8th Cir. 1995) ("[U]pon a proper application being made under 18 U.S.C. § 3122, 'the court *shall* enter an ex parte order authorizing the installation' of such a device." (emphasis in original)).

92. *In re* Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device, 846 F. Supp. 1555, 1559 (M.D. Fla. 1994); *see* Mell, *supra* note 83, at 403.

93. Susan Freiwald, *Uncertain Privacy: Communication Attributes After The Digital Telephony Act*, 69 S. CALIF. L. REV. 949, 988–89 (1996).

certification to satisfy this low bar.[94] That low standard may be appropriate in applications in which law enforcement officials are truly seeking a traditional pen register to ascertain the numbers called from a specific cell phone. However, as the few known examples of requests for authorization to employ a cell site simulator demonstrate, the use of the pen register statute to support seeking materials with a cell site simulator is more troubling.

IV. Few Available Examples of Either Motions or Court Orders Address Cell Site Simulators & Similar Devices

Very few judicial decisions address the use of these tools of electronic surveillance. One possible reason for the lack of decisions is that the government has attempted to keep its use of cell site simulator technology a secret.[95] For example, law enforcement officials often file their applications as requests for pen registers without much, if any, reference to the fact that the device to be used is a different type of electronic surveillance than the traditional pen register.[96] Moreover, when courts ask the government to provide legal authority for such electronic surveillance, pursuant to the pen register statute, the government is less than candid.[97] Finally, various government agencies, both federal and state alike, have taken measures to keep their use of cell site simulators secret. The FBI has gone so far as to require its employees to sign nondisclosure agreements to prevent them from disclosing any information about the government's use of cell site simulators.[98] There

94. *See* Bellia, *supra* note 82, at 1431 ("[T]he statute does not appear to require the judge to independently assess the factual predicate for the government's certification."); Lee, *supra* note 25, at 397 ("Pen register and trap and trace authority is also problematic in that orders are generally rubberstamped without question."). *But see In re* Application of the U.S. for an Order Authorizing the Installation & Use of a Device [Pen Register], No. 87-0831RC, 1987 WL 8946 (D. Mass. Apr. 3, 1987) (denying a pen register without prejudice due to deficiencies in the application).

95. *See* Elec. Privacy Info. Ctr. v. FBI, 933 F. Supp. 2d 42 (D.D.C. 2013) (denying the FBI's motion for a stay of deadline to provide responses to Freedom of Information Act requests regarding StingRay); Paul Ohm, *Electronic Surveillance Law and the Intra-Agency Separation of Powers*, 47 U.S.F. L. Rev. 269, 275 (2012) (discussing rumors of various types of electronic surveillance, including StingRays, that have ultimately been confirmed); Kurth & Abdel-Razzaq, *supra* note 11; Nathan Freed Wessler, *U.S. Marshals Seize Local Cops' Cell Phone Tracking Files in Extraordinary Attempt to Keep Information From Public*, ACLU (June 3, 2014, 12:13 PM), https://www.aclu.org/blog/national-security-technology-and-liberty/us-marshals-seize-local-cops-cell-phone-tracking-files (discussing the federal government's efforts to prevent disclosure of information related to the Sarasota Police Department's use of a cell site simulator).

96. *In re* Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device, 890 F. Supp. 2d 747, 747 (S.D. Tex. 2012).

97. Owsley, *supra* note 15, at 40; Pell & Soghoian, *supra* note 16, at 158.

98. Ryan Gallagher, *Judge Oks FBI Tracking Tool That Tricks Cellphones with Clandestine Signal*, Slate (May 9, 2013, 4:35 PM), http://www.slate.com/blogs/future_tense/2013/05/09/stingray_imsi_catcher_judge_oks_fbi_use_of_controversial_tool_in_daniel.html. Obviously, these nondisclosure agreements do not apply to FBI agents seeking judicial authorization. *See* Wessler, *supra*

are also allegations that the Sarasota Police Department distorted its response to the court regarding its use of a StingRay.[99]

Indeed, in one case that I heard as a federal magistrate judge, the Assistant United States Attorney ("AUSA") who appeared before me repeatedly indicated that a legal memorandum would be forthcoming, but instead filed a motion to withdraw after a month. In another case the federal prosecutor indicated that he would provide legal authority the next day, but ultimately did not provide any such support.[100] The magistrate judge hearing the case informed the AUSA that there were some problems with the application.[101] Despite providing feedback and guidance, the magistrate judge never heard from the applicant.[102]

Existing decisions reveal that the government filed such applications pursuant to the pen register statute. With the exception of one published decision, they all address the standard after the amendments in the USA Patriot Act. Additionally, few, if any, form motions and orders created by law enforcement officials exist.

A. Court Orders Addressing Applications for Digital Analyzers and Cell Site Simulators

1. The Central District of California

One of the first known decisions discussing law enforcement's use of this technology involves an application by the government for authorization to use a digital analyzer.[103] This is the only published decision addressing such electronic surveillance devices prior to the USA Patriot Act.

In this application, the government could not identify the cell phones of any of the five subjects of its narcotics investigation, but

---

note 59 (discussing the FBI's attempt to keep sealed testimony about the Tallahassee Police Department's use of a StingRay); Kurth & Abdel-Razzaq, *supra* note 11.

99. Cyrus Farivar, *Legal Experts: Cops Lying About Cell Tracking "Is a Stupid Thing to Do*," Ars Technica (June 20, 2014, 9:38 PM), http://arstechnica.com/tech-policy/2014/06/legal-experts-cops-lying-about-cell-tracking-is-a-stupid-thing-to-do.

100. *In re Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device*, 890 F. Supp. 2d at 749.

101. E-mail from Magistrate Judge, U.S. District Court for the Eastern District of Texas, to Brian Owsley (Mar. 5, 2013, 10:58 AM) (on file with author).

102. *Id.*

103. *See generally In re* Application of the U.S. for an Order Authorizing the Use of a Cellular Tel. Digital Analyzer, 885 F. Supp. 197 (C.D. Cal. 1995); *see also Fourth Amendment and the Internet: Hearing Before the Subcomm. on the Constitution of the Comm. on the Judiciary H.R.*, 106th Cong. 165–66 (2000), *available at* http://commdocs.house.gov/committees/judiciary/hju66503.000/hju66503_0.htm (prepared statement of Robert Corn-Revere, Att'y, Hogan & Hartson L.L.P.) (discussing the decision from the Central District of California).

instead sought to analyze the signals from these subjects' cell phones.[104] Specifically, the applicant indicated that the investigators would "conduct surveillance of the subjects of the investigation, and when they observe[d] a subject using a cellular telephone, they [would] turn on the digital analyzer."[105] At that time they would obtain the information related to the specific cellular telephone that the subject was using.

Although the application sought a court order for the digital analyzer pursuant to 18 U.S.C. § 3123, the government maintained that a court order was not necessary.[106] The trial court agreed, reasoning that the Fourth Amendment did not afford the subjects of a criminal investigation a reasonable expectation of privacy regarding their telephone numbers.[107] The court further explained that the pen register statute did not apply to the government's application because the statute contemplated investigation of a specific phone, whereas in this instance, law enforcement was targeting the individuals using the phones.[108]

Although the pen register statute did not apply per se, the court found that the spirit of the statute covered the intended activity. Applying the requirements of the statute, the court found the proposed order deficient. First, because the telephone numbers of the subjects of the investigation were unknown, it would be impossible to comply with the statute.[109] The court concluded that in passing the pen register statute, Congress had two principal concerns: "(1) the abusive interception of communications and (2) the accountability of law enforcement officers using advanced technology that might threaten privacy rights."[110] The trial court specifically expressed concern about the digital analyzer intercepting the "telephone numbers and calls made by others than the subjects of the investigation."[111] Additionally, because the proposed court order did not list the specific telephone numbers to be targeted by the digital analyzer, the order should have included "a

104. In re *Application for Use of a Cellular Tel. Digital Analyzer*, 885 F. Supp. at 199.

105. *Id.* at 200.

106. *Id.* at 199.

107. *Id.* (discussing Smith v. Maryland, 442 U.S. 735, 742–45 (1979)); *see* Pell & Soghoian, *supra* note 16, at 157–58.

108. In re *Application for Use of a Cellular Tel. Digital Analyzer*, 885 F. Supp. at 199–200; *see* Freiwald, *supra* note 93, at 988–89 ("The court, having refused to consider the device a pen register since it did not attach to a telephone line, found that no court order of any kind was required to use the device."); *Fourth Amendment and the Internet: Hearing Before the Subcomm. on the Constitution of the Comm. on the Judiciary H.R.*, 106th Cong. 165 (2000) (prepared statement of Robert Corn-Revere, Att'y, Hogan & Hartson L.L.P.) (noting, regarding this decision, that "[c]onsistent with the statutory language and legislative history, reviewing courts have interpreted these provisions literally, and narrowly").

109. In re *Application for Use of a Cellular Tel. Digital Analyzer*, 885 F. Supp. at 201 (discussing § 3123(b)(1)(C)).

110. *Id.* at 201.

111. *Id.*

requirement that the investigative agency maintain a time log identifying each target cellular telephone analyzed (by ESN and telephone number), together with all intercepted telephone numbers dialed or pulsed from each such telephone."[112] Because the application did not include the numbers or this requirement, the court denied the application without prejudice.[113]

2. The Southern District of Texas

a. The Use of a Cell Site Simulator in a Prison Setting

Since the enactment of the USA Patriot Act in 2001, there have been a few examples of applications for cell site simulators in federal court. In April of 2011, for example, the government filed an application for a pen register in the Southern District of Texas.[114] Specifically, the AUSA indicated that the government suspected that federal prison inmates were using cellular phones to perpetrate various federal offenses.[115] The government knew the names of the suspects, their location, and the location where they typically used their cell phones;[116] however, it did not know the phone numbers or in whose names the phones were purchased or leased.[117] To advance its investigation, federal law enforcement agents sought an order authorizing the installation of a pen register and a trap and trace device.[118] In the application, the government requested authority to use a device that could ascertain the number of any cell phones operating within a particular area, including the prison facilities.[119] According to the AUSA's statements during *ex parte* discussions, the device functioned by impersonating a cell tower, thereby receiving all of the signals sent from any nearby cellular phones.[120]

The government acknowledged that the device would capture the phone numbers of other phones that happened to be in the vicinity, but was confident in its ability to quickly winnow those numbers out and target the phones being used by the suspects.[121] The AUSA did not indicate how this winnowing process would be done. When asked about

---

112. *Id.* at 202.

113. *Id.*

114. *In re* Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device, No. 2:11-mj-00468 (S.D. Tex Apr. 6, 2011).

115. *Id.* at 1.

116. *Id.* at 2.

117. *Id.*

118. *Id.* at 1.

119. *Id.* at 2.

120. Hearing Minutes, *In re* Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device, No. 2:11-mj-00468 (S.D. Tex. May 6, 2011).

121. *Id.* at 2–3.

legal authority supporting the government's application, the Court was advised that a brief with legal support would be filed.

Instead of filing this legal brief, about a month after the application was filed, the government filed a motion to withdraw the application because prison officials had discovered and confiscated the cellular telephones that the government was trying to locate.[122] Because the application was moot, the motion to withdraw was granted.[123]

b. The Use of a Cell Site Simulator to Target a Drug Dealer

In another application before the Southern District of Texas, the government sought a pen register and a trap and trace regarding a Drug Enforcement Administration ("DEA") investigation.[124] The underlying investigation focused on an individual who was allegedly engaged in narcotics trafficking, based on an investigation of a number of years.[125] In its application, the government acknowledged that it did not know the telephone number of the cell phone used by the subject of the investigation.[126] During an *ex parte* hearing, the federal agent in charge of the investigation acknowledged that the application sought to use a StingRay device "to detect radio signals emitted from wireless cellular telephones in the vicinity of the [Subject] that identify the telephones."[127] Specifically, he explained that if the application were granted, the device would be employed from a vehicle that would be driven near the home of the subject of the investigation; that same vehicle would also follow the subject when he went other places during the period of surveillance.[128] In this manner, the agents hoped that a common cell phone number would materialize from the numbers obtained at the various surveillance-gathering locations.

The AUSA indicated "that the application was based on a standard application model and proposed order approved by the United States Department of Justice" for use by federal prosecutors.[129] During the hearing, the AUSA was unfamiliar with some case law raised during the

---

122. *See generally id.*

123. Order Granting Mot. to Withdraw, *In re* Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device, No. 2:11-mj-00468 (S.D. Tex. May 6, 2011).

124. *See generally In re* Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device, 890 F. Supp. 2d 747 (S.D. Tex. 2012); *see also* Pell & Soghoian, *supra* note 16, at 160–62.

125. *In re Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device*, 890 F. Supp. 2d at 748.

126. *Id.*

127. *Id.*; *accord* Pell & Soghoian, *supra* note 16, at 161.

128. *See In re Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device*, 890 F. Supp. 2d at 748.

129. *Id.* at 749; *see* ELECTRONIC SURVEILLANCE MANUAL, *supra* note 24, at 38–40.

discussion, but represented to the court that he would file a legal memorandum in support of his application the next day.[130] However, that legal support was never provided to the court.[131]

In its analysis of the application, the court first discussed the historical view of pen registers.[132] Next, it discussed the revised definition of a pen register based on the USA Patriot Act.[133] Notwithstanding the broader definition of a pen register in the Patriot Act, the court found that the statute and case law required that the pen register applicant be targeting a known telephone number.[134] According to the judge, "the plain language of the statute mandates that this Court have a telephone number or some similar identifier before issuing an order authorizing a pen register."[135] In other words, given the absence of a known cell phone number target, neither case law nor statutory language supported the applicability of the pen register statute to an application for a cell site simulator.

3. The Northern District of Texas

In an application filed in the Northern District of Texas in 2012, the government sought an order authorizing a pen register regarding the cellular phones used by the subject of an ongoing narcotics trafficking investigation. The alleged violations were possession with intent to distribute cocaine, marijuana, and methamphetamine in violation of 21 U.S.C. § 841 and for conspiracy to possess with intent to distribute cocaine, marijuana, and methamphetamine in violation of 21 U.S.C. § 846.[136] The ASUA represented that the subject of the investigation was using one or more unidentified cellular phones.[137] The government knew that this subject lived at one specific location and frequented another where he worked.[138] However, the government did not know the cell

130. *In re Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device*, 890 F. Supp. 2d at 749.

131. *Id.* at 749 n.1.

132. *Id.* at 749 (discussing United States v. Giordano, 416 U.S. 505, 512 n.2 (1974) and United States v. N.Y. Tel. Co., 434 U.S. 159, 161 n.1(1977)).

133. *Id.* at 749.

134. *Id.* at 750–51; *see* Gus Hosein & Caroline Wilson Palow, *Modern Safeguards for Modern Surveillance: An Analysis of Innovations in Communications Surveillance Techniques*, 74 OHIO ST. L.J. 1071, 1102 (2013).

135. *In re* Application of the U.S. for an Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, 890 F. Supp. 2d at 751 (discussing 18 U.S.C. § 3123(b)(1)(C)); Pell & Soghoian, *supra* note 16, at 161.

136. *In re* Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device (N.D. Tex. Apr. 5, 2012) (on file with author).

137. *Id.*

138. *Id.*

phone subscriber information of the persons leasing the cell phones that the subject was using.[139]

In its application, the government explained that it sought to use the pen register to simply identify the subject's telephone number, as opposed to tracking the cell phone or attempting to determine its location.[140] Consequently, the use of surveillance equipment was to be limited: "Once the identifying registration data and the number of the *Subject Telephone* is identified, utilization of the pen register . . . shall cease."[141]

The court granted the government's application; however, the judge did impose some limits on the government's use of these devices.[142] The judge mandated that the order applied only to the cell phone used by the subject, and that the cell site simulator was to be used only in the subject's vicinity to ascertain his cell phone number.[143] Additionally, the judge specifically barred the use of the cell site simulator "when the *Subject* [was] in a location in which he would have a reasonable expectation of privacy; including but not limited to: a private residence, a vehicle, or a private office."[144] Once the subject's cell phone number was determined, the government was ordered to cease using the cell site simulator.[145] The government was apparently displeased with the court's conditions and ultimately did not use a cell site simulator.[146] Indeed, the AUSA informed the magistrate judge that the restrictions were too onerous.[147]

4. The District of Maryland

In an application filed in the District of Maryland in 2012, the government sought an order relating to the cellular phones used by the subject of an ongoing narcotics trafficking investigation for alleged violations of conspiracy to distribute controlled substances.[148] Specifically, the government sought to use a device to obtain "certain unknown mobile telephone(s) presently with unknown call number(s); unknown subscriber(s); and unknown service provider(s)" used by the

139. *Id.* at 1–2.

140. *Id.* at 2–3.

141. *Id.* at 3 (emphasis in original).

142. Order Granting, *In re* Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device (N.D. Tex. Apr. 5, 2012).

143. *Id.* at 2.

144. *Id.* (emphasis in original).

145. *Id.*

146. E-mail from Magistrate Judge, U.S. District Court for the Northern District of Texas, to Brian Owsley (June 4, 2012, 11:49 AM) (on file with author).

147. *Id.*

148. *In re* Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register/Trap & Trace Device, No. [Redacted] (D. Md. Mar. [Redacted], 2012).

subject of the ongoing investigation.[149] The AUSA elaborated that "[t]he purpose of this requested order is to identify this unknown information by deploying the device to the Target Telephone(s)."[150]

The AUSA indicated that the cell site simulator would "detect radio signals emitted from wireless cellular telephones in the vicinity of the target, including the Target Telephone(s)."[151] The AUSA further explained that "[b]y determining the identifying registration data at various locations in which the subject telephone is reasonably believed to be operating, the telephone number(s) and/or subscriber identities corresponding to the Target Telephone(s) can be identified."[152] The government acknowledged that, by using the device, it would invariably capture the telephone numbers of innocent third parties.[153]

The application requested the court to order that, when the federal agents obtained information from the search, they were "to log the identity of each cellphone analyzed, together with the intercepted subscriber identities for each device."[154] Moreover, it sought an order requiring that the government "avoid the collection of data from individuals other than that of the target."[155]

Interestingly, the government asserted that the 1995 Central District of California opinion provided support for its application.[156] Although the application acknowledged that the 1995 decision was not favorable to the government, the decision provided guidance as to what any subsequent applications should contain.[157] Finally, the AUSA maintained that the application and the attached proposed order pending before the Maryland district court adhered to the dictates from the 1995 decision.[158]

5. The District of New Jersey

In an application filed in the District of New Jersey in 2012, the government sought an order authorizing a pen register and trap and trace device as well as subscriber information, pursuant to 18 U.S.C.

149. *Id.*
150. *Id.* at 2.
151. *Id.*at 3 n.4.
152. *Id.*
153. *Id.* at 3–4, 4 n.5.
154. *Id.* at 4.
155. *Id.* at 5.
156. *Id.* at 3 n.3 (citing *In re* Application of the U.S. for an Order Authorizing the Use of a Cellular Tel. Digital Analyzer, 885 F. Supp. 197 (C.D. Cal. 1995)).
157. *Id.*
158. *Id.*

§ 2703.[159] The government knew the targeted cell phone number and that it was issued by Simple Mobile through its relationship with T-Mobile.[160] Because the location of the targeted cell phone was unknown, the application also sought authorization for "the FBI to deploy mobile pen register and trap and trace equipment to determine the general location of the cellular telephone facility assigned [to the specific] telephone number."[161] The court authorized the use of this "mobile pen register equipment" "in order to determine the general location" of the cell phone.[162] However, the court limited the FBI from "us[ing] the mobile equipment, absent other authority, to locate the Target Facility once it leads them to believe that they have identified a single residence or private space within which the Target Facility may be located."[163]

6. The District of Arizona

In a criminal prosecution in the District of Arizona, the government sought the defendant, a fugitive indicted on 74 counts of mail and wire fraud, aggravated identity theft, and conspiracy.[164] "The government located and arrested Defendant, in part, by tracking the location of an aircard connected to a laptop computer that allegedly was used to perpetuate the fraudulent scheme."[165]

After the defendant's arrest, he filed a motion for disclosure of evidence, as well as additional discovery. Specifically, he sought extremely detailed information regarding the aircard, as well as the identities and training of the FBI agents capable of using this technology.[166] In support of the defendant's motion, the American Civil Liberties Union ("ACLU") filed an *amicus* brief arguing that because the AUSA seeking the original order authorizing the use of the StingRay failed "to apprise the magistrate that it intended to use a stingray, what the device is, and how it works, it prevented the judge from exercising his

159. *In re* Application of the U.S. for an Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device for the Cellular Telephone Facility Currently Assigned Telephone Number [Redacted], Mag. No. 12-3016 (D.N.J. Feb. 21, 2012).

160. *Id.* at 1.

161. *Id.*

162. *Id.* at 4.

163. *Id.*

164. *See Rigmaiden I*, 844 F. Supp. 2d 982, 987–88 (D. Ariz. 2012).

165. *Id.* "Air cards are devices that plug into a computer and use the wireless cellular networks of phone providers to connect the computer to the internet. The devices are not phones and therefore don't have the ability to receive incoming calls . . ." Kim Zetter, *Secrets of FBI Smartphone Surveillance Tool Revealed in Court Fight*, WIRED (Apr. 9, 2013, 6:30 AM), http://www.wired.com/threatlevel/2013/04/verizon-rigmaiden-aircard/all.

166. *Rigmaiden I*, 844 F. Supp. 2d at 993.

constitutional function of ensuring that warrants are not overly intrusive and all aspects of the search are supported by probable cause."[167]

The government stipulated to a number of facts related to the motion for discovery, as well as the motion to suppress. It agreed that "[t]he mobile tracking device used by the FBI to locate the aircard function[ed] as a cell-site simulator. The mobile tracking device mimicked a Verizon Wireless cell tower and sent signals to, and received signals from, the aircard."[168] Additionally, the government acknowledged that "[t]he FBI used the mobile tracking device in multiple locations," taking readings and then moving to another location to take more readings.[169]

In locating the defendant with the use of the cell site simulator device, the government indicated that "[t]he FBI never used more than a single piece of equipment at any given time."[170] Moreover, the agents using the device were on foot near the defendant's apartment.[171] During that surveillance, these agents made telephone calls to the aircard.[172] The government indicated that "[t]he mobile tracking device used to simulate a Verizon cell tower [was] physically separate from the pen register trap and trace device used to collect information from Verizon."[173] Finally, for purposes of the defendant's pending motion, the government stipulated that "[t]he tracking operation was a Fourth Amendment search and seizure."[174]

In July 2008, the government obtained a warrant pursuant to Rule 41 of the Federal Rules of Criminal Procedure from a magistrate judge in the Northern District of California authorizing the use of the StingRay device to locate the aircard.[175] In finding probable cause, the magistrate judge identified the aircard by both its specific assigned telephone number as well as its ESN.[176] In the motion to suppress, the defendant argued that the government's use of the device to track the aircard violated his Fourth Amendment rights.[177] Specifically, he argued "that the warrant is not supported by probable cause, that it lacks particularity, that the government's searches and seizures exceeded the warrant's scope, and that agents executed the warrant unreasonably

---

167. [Proposed] Brief Amici Curiae in Support of Daniel Rigmaiden's Motion to Suppress at 14, *Rigmaiden II*, No. CR 08-814-PHX-DGC, 2013 WL 1932800 (D. Ariz. May 8, 2013).

168. *Rigmaiden I*, 844 F. Supp. 2d at 995.

169. *Id.*

170. *Id.*

171. *Id.*

172. *Id.*

173. *Id.*

174. *Id.* at 995–96.

175. *Rigmaiden II*, No. CR 08-814-PHX-DGC, 2013 WL 1932800, at *14 (D. Ariz. May 8, 2013).

176. *Id.*

177. *Id.*

because they failed to comply with inventory and return requirements."[178]

The district court judge found that the agent's affidavit in support of the warrant clearly linked locating the aircard with a high likelihood that it would lead to evidence of criminal activity.[179] Furthermore, the court noted that the agent's affidavit specifically indicated that the authorized device was used to locate the aircard.[180] Next, the court concluded that the warrant was sufficiently particular based on the use of the specific telephone number and the ESN identifying the aircard.[181] Regarding any argument for privacy by the defendant, the judge concluded that the defendant did not have a legitimate expectation of privacy in light of the fact that he obtained his residence and the computers through identity theft and other fraudulent means.[182]

Regarding the scope of the warrant, defendant argued that Verizon, rather than the FBI, was authorized to search for the aircard.[183] Again, the court rejected this argument, noting that while the warrant was "not a model of clarity," it satisfied the standard mandated by Rule 41.[184] Ultimately, the court denied the motion to suppress the evidence related to the aircard in part because the defendant did not have a legitimate expectation of privacy in his aircard.[185]

7. Other Magistrate Judges Have Acknowledged Handling Cell Site Simulator Applications

Of course, the above discussion is not exhaustive, as other magistrate judges may have received applications using the pen register application and not realized that they were authorizing or denying use of a cell site simulator.[186] One magistrate judge in the Western District of Washington explained that he received a request for a TriggerFish in 2011, which he denied.[187] Similarly, a magistrate judge in the Eastern District of Texas was faced with a pen register application for a cell site simulator.[188] He indicated some concerns that he had with the request and sought some revisions, or in the alternative, some authority in

178. *Id.*
179. *Id.* at *16.
180. *Id.*
181. *Id.* at *17.
182. *Id.* at *8–9.
183. *Id.* at *18.
184. *Id.* at *19.
185. *Id.* at *33–34.
186. Soghoian, *supra* note 37.
187. E-mail from Magistrate Judge, U.S. District Court for the Western District of Washington, to Brian Owsley (May 31, 2012, 11:40 AM) (on file with author).
188. E-mail from Magistrate Judge, U.S. District Court for the Eastern District of Texas, to Brian Owsley (Mar. 5, 2013, 10:58 AM) (on file with author).

support of the requested application.[189] Ultimately, the AUSA withdrew the application.[190]

Another magistrate judge indicated that he and his colleagues in the Southern District of California routinely grant requests for cell site simulators because people do not have any expectation of privacy in their telephone numbers.[191] He did note that an authorization covered only the recording of the ESN and MIN numbers transmitted to the telecommunication providers by cell phone.[192]

B. Form Applications and Orders Drafted by Law Enforcement Agencies

In addition to these judicial examples addressing government applications to use cell site simulators, law enforcement officials have provided other examples in their training manuals.

1. The United States Attorneys' Bulletin

In a September 1997 *United States Attorneys' Bulletin*, the Electronic Surveillance Unit of the Officer of Enforcement Operations within the Criminal Division of the DOJ issued guidance regarding certain electronic surveillance techniques, including digital analyzers and cell site simulators.[193] This Bulletin explained that "[i]t is now possible for agents to capture electronically the unknown [ESN] or telephone number of a cellular telephone through the use of a device known as a *digital analyzer*."[194] It further explained that a digital analyzer "can be programmed to identify the telephone number assigned to the subject cellular telephone and telephone numbers dialed from this phone, as well as its ESN; i.e. a number assigned by the cellular telephone manufacturer and programmed into the telephone."[195] The Bulletin explicitly acknowledged that, because a digital analyzer is capable of intercepting communications as well as telephone numbers, the device "is programmed so it will not intercept cellular conversations or dialed

189. *Id.*

190. *Id.*

191. E-mail from Magistrate Judge, U.S. District Court for the Southern District of California, to Brian Owsley (May 31, 2012, 1:01 PM) (on file with author).

192. *Id.*; *see* United States v. Espudo, 954 F. Supp. 2d 1029, 1045 (S.D. Cal. 2013) (denying as moot a motion to suppress evidence obtained by a cell site simulator where the federal agent testified that the information gathered was not "utilized to further the investigation").

193. *The Office of Enforcement Operations—Its Role in the Area of Electronic Surveillance*, 45 U.S. Att'y Bull., no. 5, Sept. 1997, at 8, 11, *available at* http://www.justice.gov/usao/eousa/foia_reading_room/usab4505.pdf.

194. *Id.* at 13 (emphasis in original).

195. *Id.* at 13–14.

numbers when it is used for the limited purpose of seizing ESNs and/or the cellular telephone's number."[196]

The Bulletin also discussed cell site simulators, explaining that they "can provide agents with a cellular telephone's ESN and mobile identification number ('MIN,' which contains the cellular telephone number and other information related to the operation of the phone)."[197] Next, it elaborated that cell site simulators:

> [S]imulate[] some of the activities of a cellular service provider's cell site transmitter, albeit in a much smaller area, and allow[] agents to query cellular phones for their ESNs and MINs through "autonomous registration," an activity a cell site transmitter normally conducts to identify cellular phones operating within its cell or area.[198]

Finally, the Bulletin discussed that as with "a real cell site transmitter, the [cell site simulator] can determine ESNs and MINs of cellular phones that are 'powered up' or turned on. (The phone need *not* be in a 'use' mode; the information can be obtained unbeknownst to the cellular phone user.)"[199]

The Bulletin discussed that both digital analyzers and cell site simulators:

> [C]an capture the cell site codes identifying the cell location and geographical sub-sector from which the cellular telephone is transmitting; the call's incoming or outgoing status; the telephone numbers dialed (pen register order required); and the date, time, and duration of the call. This cell site data is transmitted continuously from a cellular telephone (not by the user) as a necessary part of call direction and processing.[200]

Each telecommunications provider "uses this information to connect with the account in order to direct calls, and constantly reports to the customer's telephone a readout regarding the signal power, status, and mode of the telephone."[201]

2. The Department of Justice Electronic Surveillance Manual

In 2005, the DOJ published an *Electronic Surveillance Manual* to provide guidance to its attorneys throughout the country. Specifically, the *Electronic Surveillance Manual* "sets forth the procedures established by the Criminal Division of the Department of Justice to obtain authorization to conduct electronic surveillance."[202] The manual, last revised in 2005, discusses digital analyzers in a section concerning

196. *Id.* at 14.
197. *Id.*
198. *Id.*
199. *Id.* (emphasis in original).
200. *Id.*
201. *Id.*
202. ELECTRONIC SURVEILLANCE MANUAL, *supra* note 24, at ii.

pen registers and trap and trace devices.[203] It explicitly cautions the need for a court order prior to using a cell site simulator:

> Because section 3127 of Title 18 defines pen registers and trap and trace devices in terms of recording, decoding or capturing dialing, routing, addressing, or signaling information, a pen register/trap and trace order must be obtained by the government before it can use its own device to capture the ESN or MIN of a cellular telephone, even though there will be no involvement by the service provider.[204]

This determination by the DOJ, that a device used only to obtain a MIN requires a court order, indicates that a device used to ascertain the telephone number would also require a court order.

In the *Electronic Surveillance Manual*, the DOJ explained that "[l]aw enforcement possesses electronic devices that allow agents to determine the location of certain cellular phones by the electronic signals that they broadcast."[205] Specifically, a cell site simulator's "equipment includes an antenna, an electronic device that processes the signals transmitted on cell phone frequencies, and a laptop computer that analyzes the signals and allows the agent to configure the collection of information."[206]

The DOJ does not describe a device used to ascertain a phone number as a pen register. However, it demonstrates a belief that the same legal standards apply to such devices. The point is made explicit in the model form application and proposed order for a TriggerFish, a digital analyzer.[207] The caption for the application reads "In the Matter of the United States of America for an Order Authorizing the Installation and Use of a Pen Register."[208] Moreover, the caption on the proposed order reads similarly.[209]

3. The District of Arizona Form

In 2012, the Acting United States Attorney for the District of Arizona created a form application to guide attorneys in that office in

---

203. *Id.* at 38–41.

204. ELECTRONIC SURVEILLANCE MANUAL, *supra* note 24, at 41. The MIN used to be the same as the assigned cell phone number. United States v. O'Shield, No. 97-2493, 1998 WL 104625, at *1 n.1 (7th Cir. Mar. 6, 1998) (per curiam) (unpublished table decision); United States v. Bailey, 41 F.3d 413, 415 (9th Cir. 1994). Pursuant to Federal Communications Commission policy, these numbers are now separate. Cellular Telecomms. Indus. Ass'n's Petition for Forbearance from Commercial Mobile Radio Servs. No. Portability Obligations & Tel. No. Portability, 14 FCC Rcd. 3092, 3105 (1999); *see* Pinney v. Nokia, Inc., 402 F.3d 430, 439–40 (4th Cir. 2005).

205. *Id.* at 44.

206. *Id.*; *compare with* Valentino-Devries, *supra* note 49.

207. ELECTRONIC SURVEILLANCE MANUAL, *supra* note 24, at 171–74.

208. *Id.* at 171.

209. *Id.* at 173.

requesting ESN identification numbers.[210] In the form application, the AUSA sought a court order "pursuant to 18 U.S.C. §§ 3122 and 3123, authorizing law enforcement to use an electronic serial number identifier to collect non-content wireless signaling information."[211] The caption on the application reads, "In the Matter of the Application of the United States of America for an Order Authorizing the Use of a Mobile Number Recorder to Collect Non-Content Signaling Information from Cellular Telephones."[212] Although the form anticipates that the requesting officials have the name of a subject of the investigation, it does not anticipate them having the cellular telephone numbers used by the subject or his drug trafficking organization, assuming the case pertains to drug trafficking.[213] The application explains that a "Mobile Number Recorder . . . is an instrument that will decode and/or record non-content signaling information transmitted by a cellular telephone within a limited radius to determine the unique numeric identifiers of the telephone or telephones."[214] The form indicates that agents seek to use the Mobile Number Recorder in conjunction with traditional physical surveillance on the subject, such as by tracking the subject in an unmarked van, to obtain telephone numbers.[215]

In support of the application, the government must certify the relevance of the telephone numbers sought.[216] The form acknowledges that the mobile number recorder will gather telephone numbers unrelated to the subject, but asserts that these unrelated numbers will not be used by the investigating agents.[217] Additionally, it acknowledges that the device might also gather dialed digit information and posits that such information will be usable by the government pursuant to the pen register statute.[218] Next, the application contains blanks in which the government is to provide the specific criminal offenses that the subject allegedly committed, as well as specific facts in support of the application.[219] The government notes that it does not need to provide "specific and articulable facts" in support of its application because it will

---

210. U.S. ATTORNEY'S OFFICE, DISTRICT OF ARIZ., APPLICATION FOR USE OF AN ELECTRONIC SERIAL NUMBER IDENTIFIER [hereinafter ARIZONA FORM APPLICATION] (2012) (on file with author). Acting United States Attorney Ann Birmingham Scheel served until July 3, 2012, when the new United States Attorney was sworn in. *See Meet the U.S. Attorney*, U.S. DEP'T OF JUSTICE, http://www.justice.gov/usao/
az/meettheattorney.html (last visited Dec. 14, 2014).

211. ARIZONA FORM APPLICATION, *supra* note 210, at 1.

212. *Id.*

213. *Id.*

214. *Id.*

215. *Id.* at 1–2.

216. *Id.* at 2.

217. *Id.* at 4.

218. *Id.* at 4–5.

219. *Id.* at 5.

simply be using the pen register statute to obtain the subject's cell phone numbers with the mobile number recorder.[220]

The government also included, in this package to attorneys, a memorandum in support of its position. In the memorandum, the government argues that the mobile number recorder falls within the pen register statute as it is a recording of signaling information.[221] The memorandum also discusses the difference in the pen register definition in the ECPA with the amendment in the USA Patriot Act.[222] The government also argues that the Fourth Amendment does not apply to the use of a mobile number recorder.[223]

The memorandum also provides an argument against the pen register statute's applicability to the mobile number recorder.[224] Specifically, it notes that any court order must "include[] the number or other identifier."[225] The government acknowledges that, since the 2001 amendment, "no court has held that a device like the one in this case falls within the statutory definition of a pen register."[226] Instead, it addresses the fact that at least one court viewing the 2001 amendments simply focused on applying the pen register statute to e-mails.[227] Consequently, that court determined that a "pen register must still be tied to an actual number or attempted phone call."[228]

The government also provided a proposed order to grant its application.[229] The proposed order follows the rationale provided by the application.[230]

4. The Los Angeles Police Department Form

At least one city has also developed form materials for use by its law enforcement officers. On September 29, 2012, Donal Brown, an editor at the First Amendment Coalition, filed a California Public Records Act Request with the Los Angeles Police Department ("LAPD") for information regarding the use of devices to track and identify a cellular

220. *Id.* at 6.

221. *Id.* at 9.

222. *Id.* at 10.

223. *Id.* at 13–14 (discussing Smith v. Maryland, 442 U.S. 735 (1979) and United States v. Forrester, 495 F.3d 1041, 1049–50 (9th Cir. 2007)).

224. *Id.* at 11.

225. *Id.* (quoting 18 U.S.C. § 3123(b)(1)(C)).

226. *Id.*

227. *Id.* at 11–12 (discussing *In re* Application for Pen Register & Trap/Trace Device with Cell Site Location Authorization, 396 F. Supp. 2d 747, 761–62 (S.D. Tex. 2005)).

228. *Id.* at 12 (discussing In re *Application for Pen Register & Trap/Trace Device*, 396 F. Supp. 2d at 762).

229. *Id.* at 13–15.

230. *Id.*

phone's IMSI.[231] Among the various requests, Brown sought "[a] copy of any LAPD internal policies, guidelines or standards for police use of an IMSI device" or in lieu of such records "all other records sufficient to show the policies, guidelines or standards in effect for LAPD use of an IMSI device."[232] Next, he requested "[r]ecords sufficient to show whether judicial authorization is obtained for LAPD deployment and use of an IMSI device and the type of judicial authorization obtained."[233] He also asked for "[r]ecords sufficient to show, for the time period June 1 [to] Sept. 30, 2012, the frequency of LAPD's deployment and use of an IMSI device," as well as, for the same time period, "[r]ecords sufficient to show . . . all LAPD uses of an IMSI device in which LAPD personnel eavesdropped on conversation."[234] Finally, he requested "[r]ecords sufficient to identify all prosecutions or other judicial proceedings initiated by the LAPD or LA District Attorney during 2011 in which information was filed in, or furnished to, the Superior Court (LA County) derived from LAPD's use of an IMSI device."[235] Brown asked that a response be provided within ten days.[236]

On December 14, 2012, Officer Martin Bland, the Officer-in-Charge of the Discovery Section within the Legal Affairs Division of the LAPD, responded to Brown's records request.[237] With respect to the first three requests, Bland indicated that he would make documents available after Brown paid the duplicating fee.[238] Bland then acknowledged that, "[d]uring the time period in your request, 21 cell phone numbers were subjected to the deployment of an IMSI," but "there were no uses of an IMSI device that involved the eavesdropping of conversations."[239] Finally, Bland declined to provide any information in response to the request regarding prosecutions involving an IMSI device because "there is no centralized repository for records (or information) responsive to [the] request," which made the request "significantly and unduly burdensome."[240]

---

231. Letter from Donal Brown, Editor, First Amendment Coal., to Martin Bland, Officer-in-Charge, Discovery Section, L.A. Police Dep't (Sept. 29, 2012) (citing CAL. GOV. CODE § 6250, *et seq.*), *available at* firstamendmentcoalition.org/wp-content/uploads/2013/03/LAPD-CPRA.pdf.

232. *Id.*

233. *Id.*

234. *Id.*

235. *Id.*

236. *Id.*

237. Letter from Martin Bland, Officer-in-Charge, Discovery Section, L.A. Police Dep't, to Donal Brown, Editor, First Amendment Coal. (Dec. 14, 2012), *available at* firstamendmentcoalition.org/wp-content/uploads/2013/03/LAPD-CPRA.pdf.

238. *Id.*

239. *Id.*

240. *Id.* (citing CAL. GOV. CODE § 6255).

On December 28, 2012, Bland provided Brown with thirty-one pages of records responsive to his request.[241] Notably, there was an October 16, 2012 memorandum to all Commanding Officers explaining that "[t]he law regarding the use of cellular and GPS tracking is evolving. Protocols governing cellphone tracking requests are necessary to ensure Department personnel are abiding by the most current case law."[242] Consequently, the memorandum mandated that "[a]ll requests for cellular tracking, made concurrent with an investigation (whether by use of a court order or under an exigent circumstances process), shall be directed through [the Real-Time Analysis and Critical Division]."[243]

In the December 28, 2012 letter from Bland to Brown, Bland provided an explanation of the statutory basis and procedures for requesting applications and court orders that use a "cell phone tracking system for identifying" a cell phone's IMSI, as well as forms for applications and orders.[244] Notably, in response to Brown's request, Bland turned over an LAPD form application addressing requests for authorization of an IMSI device in the Superior Court for the County of Los Angeles.[245] The caption reads, "In the Matter of the Application of the People of the State of California for an Order Authorizing the Use of a Pen Register and a Trap-and-Trace Device on Telephone Line Currently Designated by Telephone Number," with a blank space to fill in the specific telephone number.[246] The application sought to distinguish between a telephone number and a telephone line because it maintained that the pen register statute was "defined with respect to telephone lines" as opposed to telephone numbers.[247] The application contained a section to be filled in by the police officer indicating the probable cause that supported the request.[248]

---

241. Letter from Martin Bland, Officer-in-Charge, Discovery Section, L.A. Police Dep't, to Donal Brown, First Amendment Coal. (Dec. 28, 2012), *available at* firstamendmentcoalition.org/wp-content/uploads/2013/03/LAPD-CPRA.pdf.

242. Memorandum from Kirk J. Albanese, Chief of Detectives, L.A. Police Dep't & Stephen R. Jacobs, Chief of Staff, L.A. Police Dep't to All Commanding Officers (Oct. 16, 2012), *available at* firstamendmentcoalition.org/wp-content/uploads/2013/03/LAPD-CPRA.pdf. Indeed, earlier that year, the Supreme Court had concluded that the attachment of a GPS tracking device to the defendant's car, whereby the government monitored its movement on public streets, constituted a Fourth Amendment search and affirmed the suppression of the resulting evidence. *See* United States v. Jones, 132 S. Ct. 945, 964 (2012).

243. Memorandum from Kirk J. Albanese & Stephen R. Jacobs to All Commanding Officers, *supra* note 242.

244. Letter from Martin Bland to Donal Brown, *supra* note 241.

245. *Id.*

246. *Id.*

247. *Id.*

248. *Id.*

With this form application, the LAPD also provided a proposed order.[249] In support of its recommendation, the LAPD proposed citing 18 U.S.C. § 2703(d)[250] as the statutory authority for the order, notwithstanding the fact that the form application is characterized as a pen register request.[251]

V. THE DEVELOPMENT OF FOURTH AMENDMENT JURISPRUDENCE

In order to understand the applicability of the Fourth Amendment to the government's applications seeking authorization of cell site simulators, one must understand the history of the Fourth Amendment. Fourth Amendment jurisprudence developed from a fairly narrow property-centric interpretation to a more flexible standard based on reasonable expectations. This more flexible standard should be reassessed in order to ensure that cell phone users have privacy from governmental intrusions into their cell phones.

A. HISTORICALLY, THE FOURTH AMENDMENT WAS PROPERTY-CENTRIC

To better understand the current state of Fourth Amendment jurisprudence, it is important to understand a little about where we started. In light of disputes with the British authorities, the founding fathers sought to ensure that people in the newly formed country would be secure from discretionary governmental intrusions in their lives.[252] The Fourth Amendment provides that it is "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[253] It further mandates that "no

249. *Id.* at 11–13.

250. 18 U.S.C. § 2703(c)(2) (In the Stored Communications Act, Congress authorized law enforcement officials to obtain telecommunications customer records, including "name; address; local and long distance telephone connection records, or records of session times and durations; length of service (including start date) and types of service utilized; telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and means and source of payment for such service (including any credit card or bank account number)."); *accord In re* § 2703(d) Order, 787 F. Supp. 2d 430, 436 (E.D. Va. 2011); *see In re* Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d), 157 F. Supp. 2d 286, 288 (S.D.N.Y. 2001) (a § 2703 order authorized law enforcement officials to obtain "the subscriber's name, home address, telephone number, e-mail address and any other identifying information [the provider] may have, such as date of birth, social security number, driver's license number and billing information"). For a court to issue an order pursuant to § 2703(d), the government must demonstrate "*specific and articulable facts* showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are *relevant and material to an ongoing criminal investigation*." 18 U.S.C. § 2703(d) (2013) (emphasis added).

251. Letter from Martin Bland to Donal Brown, *supra* note 241, at 11–13.

252. Casey, *supra* note 77, at 983.

253. U.S. CONST. amend IV.

Warrants shall issue, but upon probable cause."[254] Consequently, the threshold matter in Fourth Amendment jurisprudence "is whether a specific action or intrusion by the government constitutes a 'search' within the meaning of the Amendment."[255]

Historically, the Fourth Amendment was viewed to safeguard citizens against search of their homes, persons, and papers based on a right of property. Many scholars have posited that Fourth Amendment jurisprudence was based on a theory of trespass.[256] One scholar further explained that this trespass theory is rooted in the landmark pre-constitution decision of *Entick v. Carrington*.[257] However, Orin Kerr recently asserted that he and others had it wrong in viewing Fourth Amendment theory as having its historical foundation in trespass.[258]

In one of the first Supreme Court decisions to address the Fourth Amendment, the defendant challenged the use of his records, seized without a warrant, to convict him for failure to pay customs duties.[259] In *Boyd*, the Court addressed the question of "compulsory production of a man's private papers, to be used against him in a proceeding to forfeit his property for alleged fraud against the revenue laws . . . [and whether that constituted] an '*unreasonable* search and seizure' within the meaning of the Fourth Amendment."[260] In concluding that the trial court erred in requiring the production of the defendant's papers, the Court looked to early colonial history as well as English history, including the decision in *Entick*, finding that the entering and searching of the home constituted a trespass.[261]

---

254. *Id.*; *see* FED. R. CRIM. P. 41 (addressing the issuance of warrants, including for the seizure of electronically stored information).

255. Casey, *supra* note 77, at 983.

256. *See, e.g.*, Susan W. Brenner, *The Privacy Privilege: Law Enforcement, Technology, and the Constitution*, 7 J. TECH. L. & POL'Y 123, 150 (2002) ("When the Fourth Amendment was adopted, the protection against invasions of privacy lay in trespass law . . . ."); Jace C. Gatewood, *Warrantless GPS Surveillance: Search and Seizure—Using the Right to Exclude to Address the Constitutionality of GPS Tracking Systems Under the Fourth Amendment*, 42 U. MEM. L. REV. 303, 333–34 (2011); Lewis R. Katz, *In Search of a Fourth Amendment for the Twenty-first Century*, 65 IND. L.J. 549, 556 n.36 (1990) ("Linking the fourth amendment to its historical context, the Supreme Court during the pre-*Katz* era allowed the law of trespass to control the outcome whenever it was claimed that government had conducted a 'search.'"); David E. Steinberg, *The Uses and Misuses of Fourth Amendment History*, 10 U. PA. J. CONST. L. 581, 583 (2008) ("Historical sources indicate that the Framers were focused on a single, narrow problem: physical trespasses into houses by government agents.").

257. (1765) 95 Eng. Rep. 807 (K.B.); Katz, *supra* note 256, at 556 n.36.

258. Orin S. Kerr, *The Curious History of Fourth Amendment Searches*, 2012 SUP. CT. REV. 67, 69 (2012); *see* Fabio Arcila, Jr., *GPS Tracking Out of Fourth Amendment Dead Ends:* United States v. Jones *and the* Katz *Conundrum*, 91 N.C. L. REV. 1, 21–22 (2012) ("*Katz* famously moved search jurisprudence to a privacy model. It did so by rejecting the property-centric Fourth Amendment model that had previously controlled, and which the Court had applied in *Olmstead v. United States*.").

259. Boyd v. United States, 116 U.S. 616, 618 (1886).

260. *Id.* at 622 (emphasis in original).

261. *Id.* at 625–28.

In *Olmstead v. United States*,[262] the Supreme Court considered a challenge to information that federal agents obtained from wiretapping the telephones within the homes of targets of a criminal investigation. Chief Justice Howard Taft made clear that the wiretapping was "made without *trespass* upon any property of the defendants" because the line that was tapped was "made in the basement of the large office building."[263] Nonetheless, he stressed that "[t]he well-known historical purpose of the Fourth Amendment, directed against general warrants and writs of assistance, was to prevent the use of governmental force to search a man's house, his person, his papers, and his effects, and to prevent their seizure against his will."[264] In many regards, the applied approach was a plain language interpretation of the amendment. Indeed, Chief Justice Taft distinguished *Hester v. United States*,[265] in which he acknowledged that there was a trespass on defendant's property, but ultimately "no search of person, house, papers, or effects."[266] In dissent, however, Justice Louis Brandeis famously cautioned that the Fourth Amendment protected citizens against "invasion of 'the sanctities of a man's home and the privacies of life.'"[267]

In *Goldman v. United States*,[268] the Supreme Court considered federal agents' use of a detectaphone against a wall to listen and assist in the recording of defendants' conversation within one defendant's office on the other side of the wall. The Court specifically held "what was heard by the use of the detectaphone was not made illegal by trespass or unlawful entry."[269] Instead, the only trespass occurred when agents actually entered the defendant's office to install another device that ultimately did not function properly and provided no information.[270] As in *Olmstead*, the dissents argued for individual privacy interests. For example, Chief Justice Harlan Fiske Stone and Justice Felix Frankfurter wrote simply:

> Had a majority of the Court been willing to overrule the *Olmstead* case, we should have been happy to join them. But as they have

---

262. 277 U.S. 438, 455 (1928).

263. *Id.* at 457 (emphasis added); *see* Henry F. Fradella, et al., *Quantifying* Katz: *Empirically Measuring "Reasonable Expectations of Privacy" in the Fourth Amendment Context*, 38 AM. J. CRIM. L. 289, 325 (2011) ("The majority rested its decision on the premise that since the wiretapping involved no physical trespass onto the defendants' property, there had been no Fourth Amendment violation.").

264. *Olmstead*, 277 U.S. at 463.

265. 265 U.S. 57, 59 (1924) (holding that defendant's illicit whiskey discovered by revenue officers in an open field on the property of the defendant's father's did not violate the Fourth Amendment); *see* United States v. Karo, 468 U.S. 705, 712–13 (1984) ("technical trespass" in applying the beeper was insufficient to establish a Fourth Amendment violation).

266. *Olmstead*, 277 U.S. at 465.

267. *Id.* at 473 (Brandeis, J., dissenting) (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

268. 316 U.S. 129 (1942).

269. *Id.* at 134.

270. *Id.* at 134–35.

> declined to do so, and as we think this case is indistinguishable from *Olmstead*'s, we have no occasion to repeat here the dissenting views in that case with which we agree.[271]

Similarly, Justice Frank Murphy dissented, noting an individual's "right of personal privacy guaranteed by the Fourth Amendment."[272]

B. In *Katz*, the Supreme Court Established the Reasonable Expectation of Privacy Analysis

Regardless of whether one views the development of Fourth Amendment jurisprudence through the prism of property rights, a trespass theory, or a literalist construction, after *Katz v. United States*,[273] the paradigm shifted. In *Katz*, the Supreme Court held that a listening device that recorded the defendant's conversation while he talked in a public telephone booth violated the Fourth Amendment. Justice Stewart Potter explained that Katz, by entering the telephone booth and closing the door before engaging in his telephone call, evidenced an attempt and a belief that his conversation would be private.[274] Justice Potter then elaborated that "[t]o read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication."[275] Finally, he determined that "[t]he 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."[276] Interestingly, the phrase "reasonable expectation of privacy," which has been the lasting impact of *Katz*, is not from Justice Stewart's majority opinion, but instead from a concurring opinion by Justice Harlan.[277]

This "reasonable expectation of privacy" standard was reiterated and adopted by a majority of the Supreme Court in *Terry v. Ohio*.[278] In elaborating on this standard, the Court explained, in *United States v.*

---

271. *Id.* at 136 (Stone, C.J. & Frankfurter, J., dissenting).

272. *Id.* (Murphy, J., dissenting).

273. 389 U.S. 347 (1967).

274. *Id.* at 352; *see* Owsley, *supra* note 15, at 10 (discussing *Katz*). *But see* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 Mich. L. Rev. 801, 821 (2004) (the question of "[e]xactly *why* the user of the phone booth was constitutionally entitled to his privacy was left to the reader's imagination") (emphasis in original).

275. *Katz*, 389 U.S. at 352.

276. *Id.* at 353.

277. *Id.* at 360 (Harlan, J., concurring) ("I join the opinion of the Court, which I read to hold only . . . that an enclosed telephone booth is an area where, like a home, and unlike a field, a person has a constitutionally protected reasonable expectation of privacy . . . ."). (citations omitted); *see* Casey, *supra* note 77, at 988 (discussing Justice Harlan's concurrence).

278. 392 U.S. 1, 9 (1968) ("We have recently held that 'the Fourth Amendment protects people, not places' . . . and wherever an individual may harbor a reasonable 'expectation of privacy.'") (quoting *Katz*, 389 U.S. at 351; 389 U.S. at 361 (Harlan, J., concurring)).

Jacobsen,[279] that "[a] 'search' occurs when an expectation of privacy that society is prepared to consider reasonable is infringed."[280] In the post-*Katz* world we are left to ponder what reasonable expectation of privacy, if any, cell phone users have as it relates to the government's use of cell site simulators.

Orin Kerr has posited that while "the phrase 'reasonable expectation of privacy' is notoriously murky, much of the Supreme Court's case law on the reasonable expectation of privacy test can be understood as distinguishing between inside and outside surveillance."[281] In an earlier article he echoed this theme: "Although the phrase 'reasonable expectation of privacy' sounds mystical, in most (though not all) cases, an expectation of privacy becomes 'reasonable' only when it is backed by a right to exclude borrowed from real property law."[282] He distinguished between inside and outside by elaborating that governmental conduct breaches a reasonable expectation of privacy when the surveillance exposes private, enclosed spaces, such as homes, cars, or packages.[283] On the other hand, Patricia Bellia has maintained:

> The main constitutional question is whether one retains a reasonable expectation of privacy in communications stored with a third party, such that acquisition of these communications constitutes a 'search' within the meaning of the Fourth Amendment. I call into question the prevailing assumption that an expectation of privacy is lacking when a service provider holds communications on a user's behalf.[284]

In *Smith v. Maryland*, the Supreme Court considered whether there were any privacy rights in the information that a pen register captures from a landline telephone.[285] The Court held that the use of a pen register to obtain the telephone numbers dialed was not a Fourth Amendment search because the telephone user had "no actual expectation of privacy in the phone numbers he dialed."[286] However, the Court's decision is a very narrow one and addresses pen register technology from the 1960s. Most importantly, the pen register at issue simply recorded a list of telephone numbers that were dialed from a *landline* telephone.[287] Indeed, the decision was issued a decade before

279. 466 U.S. 109 (1984).

280. *Id.* at 113 (citations omitted); *see* Rakas v. Illinois, 439 U.S. 128, 144 n.12 (1978) ("Legitimation of expectations of privacy by law must have a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society.").

281. Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 316 (2012).

282. Kerr, *supra* note 274, at 809–10.

283. Kerr, *supra* note 281, at 316–17.

284. Bellia, *supra* note 82, at 1382.

285. 442 U.S. 735 (1979).

286. *Id.* at 745–46.

287. *See* Casey, *supra* note 77, at 993 ("The Court's description of a 1971 pen register [in *Smith*] highlights the dramatic change in the capability of a 2007 pen register.").

the cell phone became ubiquitous. The *Smith* Court did not address the vast amount of information that the government routinely seeks these days in pen register applications for cellular telephones, including the time, date, and duration of any cell phone call as well as the physical location from which the call was made.[288] In other words, the analysis of *Smith v. Maryland*, predicated on the information obtained on a landline telephone, does not apply to the information that is obtainable through a pen register for a cell phone today.[289] The typical consumer does not expect that all of this data is widely available to the government any time that it simply asks for it.[290] The uproar and outrage over the breaches by the National Security Agency ("NSA") further demonstrate that there is no reasonable expectation that this information is anything but private.[291]

In *Georgia v. Randolph*,[292] the Supreme Court addressed a Fourth Amendment challenge in which the defendant sought to suppress cocaine obtained during a search of his home that resulted in this conviction for possession of cocaine. Specifically, when police officers responded to a call about a domestic dispute at the residence, the defendant's estranged wife indicated to them that her husband had narcotics in their home.[293] Although the defendant expressly refused to consent to the search of his home when officers asked, they then obtained consent from his wife.[294] In the majority opinion written by Justice David Souter, the Court held that the warrantless search was unreasonable in light of the defendant's express refusal to consent to the search.[295]

In a dissenting opinion joined by Justice Antonin Scalia, Chief Justice John Roberts took issue with the notion that defendant had a

---

288. 442 U.S. at 736 n.1; *see* Casey, *supra* note 77, at 992 ("Significantly, the device did not 'overhear' oral communications, and was not capable of determining whether or not the call was completed.").

289. *See* California v. Riley, 134 S. Ct. 2473, 2493 (2014) (distinguishing *Smith* in part because "call logs typically contain more than just phone numbers").

290. *See* Marc McAllister, *The Fourth Amendment and New Technologies: The Misapplication of Analogical Reasoning*, 36 S. ILL. U. L.J. 475, 522 (2012) ("[R]ulings associated with more traditional forms of surveillance do not always comport with society's actual expectations of privacy and often fail to account for relevant differences between the analogized cases.").

291. Scott Shane & Colin Moynihan, *Drug Agents Use Vast Phone Trove, Eclipsing N.S.A.'s*, N.Y. TIMES, Sept. 2, 2013, at A1; John Shiffman & Kristina Cooke, *Exclusive: U.S. Directs Agents to Cover up Program Used to Investigate Americans*, REUTERS (Aug. 5, 2013, 3:25 PM), http://www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805.

292. 547 U.S. 103 (2006).

293. *Id.* at 107; *see* Jeremy A. Blumenthal et al., *The Multiple Dimensions of Privacy: Testing Lay "Expectations of Privacy,"* 11 U. PA. J. CONST. L. 331, 334 (2009).

294. *Randolph*, 547 U.S. at 107.

295. *Id.* at 122–23 ("This case invites a straightforward application of the rule that a physically present inhabitant's express refusal of consent to a police search is dispositive as to him, regardless of the consent of a fellow occupant. Scott Randolph's refusal is clear, and nothing in the record justifies the search on grounds independent of Janet Randolph's consent.").

reasonable expectation of privacy in his home once he shared that home with another person, in this case his wife.[296] Chief Justice Roberts continued by explaining that there are a large number of situations that might lead to various and different social expectations.[297] Ultimately, he asserted that custom and "widely shared social expectation" were not a basis for evaluating a search pursuant to the Fourth Amendment.[298]

Chief Justice Roberts' visceral reaction to social expectation in *Georgia v. Randolph* is interesting when compared to his response to the Government's oral argument in *United States v. Jones*. In *Jones*, the Court dealt with whether the government could place a GPS tracking device on the vehicle of a subject of a criminal investigation without a warrant. During oral argument, Chief Justice Roberts had this exchange with the Deputy Solicitor General:

> CHIEF JUSTICE ROBERTS: You think there would also not be a search if you put a GPS device on all of our cars, monitored our movements for a month? You think you're entitled to do that under your theory?
>
> MR. DREEBEN: The Justices of this Court?
>
> CHIEF JUSTICE ROBERTS: Yes.
>
> (Laughter.)
>
> MR. DREEBEN: Under our theory and under this Court's cases, the Justices of this Court when driving on public roadways have no greater expectation of —
>
> CHIEF JUSTICE ROBERTS: So, your answer is yes, you could tomorrow decide that you put a GPS device on every one of our cars, follow us for a month; no problem under the Constitution?
>
> MR. DREEBEN: Well, equally, Mr. Chief Justice, if the FBI wanted to, it could put a team of surveillance agents around the clock on any individual and follow that individual's movements as they went around on the public streets.[299]

Put simply, Chief Justice Roberts appeared to address the reasonable expectations of privacy as it personally relates to him and the other members of the Court. Roberts was seemingly concerned about the real possibility that someone could legally engage in this type of

---

296. *Id.* at 128 (Roberts, C.J., dissenting) ("The correct approach to the question presented is clearly mapped out in our precedents: The Fourth Amendment protects privacy. If an individual shares information, papers, *or places* with another, he assumes the risk that the other person will in turn share access to that information or those papers *or places* with the government.") (emphasis in original).

297. *Id.* at 129–30 (Roberts, C.J., dissenting).

298. *Id.* at 131 (Roberts, C.J., dissenting); *see* Fradella et al., *supra* note 263, at 293 ("[J]udges make no attempt to discern actual societal opinions when adjudicating Fourth Amendment disputes."); Blumenthal et al., *supra* note 293, at 332 (judges often "made explicit psychological assumptions about perceptions and expectations of privacy, assumptions that are not necessarily supported by empirical findings").

299. Transcript of Oral Argument at 9–10, United States v. Jones, 132 S. Ct. 945 (2012) (No. 10-1259); *see* Arcila, *supra* note 258, at 40 (discussing this exchange).

surveillance of his vehicle without judicial authorization.[300] While the majority decision, which he joined, focused on a Fourth Amendment violation based on a trespass theory, he implied that the Supreme Court Justices (and others) had an expectation of some privacy.[301] The reason for this expectation could arguably be based on the personal nature of one's vehicle and daily travels. Still, he argued there was no expectation of privacy if law enforcement officials arrived at his residence and sought to search his home over his objections if his wife gave them express authority.[302] Possibly, he was more certain that he and his wife are of one mind regarding such a potential intrusion than the possibility that a tracking device could be placed on his vehicle.

In *Jones*, Justice Sonia Sotomayor discussed both *Smith* and *Miller* in arguing that the third-party doctrine needs to be reconsidered: "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[303] She continued by asserting that the approach established in *Miller* and *Smith* "is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks" including revealing information based on their cell phone usage.[304] In criticizing Justice's Scalia's opinion in *Jones*, Justice Samuel Alito noted that the issue was not the physical trespass, but the lengthy and intrusive nature of the electronic surveillance.[305] He continued by positing that the old method of Fourth Amendment analysis may be inapplicable to the new issues raised by electronic surveillance.[306] Similarly, the Court in *Kyllo v. United States*[307] cautioned that "[w]hile the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development."[308]

Since the Supreme Court decided *Jones*, one federal appellate court has addressed the issue of whether the use of warrantless cell site location information violates the Fourth Amendment. The Eleventh Circuit concluded that "it cannot be denied that the Fourth Amendment

---

300. Transcript of Oral Argument, *Jones*, 132 S. Ct. 945 (No. 10-1259).

301. A significant majority of individuals surveyed have a reasonable expectation of privacy from electronic tracking of one's vehicle. *See* Fradella et al., *supra* note 263, at 325.

302. *Randolph*, 547 U.S. at 120.

303. *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring) (citing Smith v. Maryland, 442 U.S. 735, 742 (1979); United States v. Miller, 425 U.S. 435, 443 (1976)).

304. *Id.*

305. *Id.* at 961 (Alito, J., concurring in judgment).

306. *Id.* at 962.

307. 533 U.S. 27 (2001).

308. *Id.* at 36. *But see* City of Ontario v. Quon, 560 U.S. 746, 759 (2010) ("The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."); *see also* Owsley, *supra* note 15, at 11.

protection against unreasonable searches and seizures shields the people from the warrantless interception of electronic data or sound waves carrying communications."[309] The court continued with an analysis of the three decisions in *Jones* and noted that the *Katz* privacy test is still applicable.[310] Ultimately, the Eleventh Circuit held "that cell site location information is within the subscriber's reasonable expectation of privacy" and that "obtaining of that data without a warrant is a Fourth Amendment violation."[311]

Most recently, in *Riley v. California*, the Supreme Court addressed whether evidence obtained by police from a defendant's cell phone during a warrantless search subsequent arrest violated the Fourth Amendment.[312] In the first of the consolidated cases, David Riley was stopped by police officers for a routine traffic stop and then subsequently arrested after his car was impounded and a search revealed firearms.[313] During his arrest, the officers seized his smart phone from his pants pocket and searched it, thereafter concluding that he was a member of a street gang.[314] The prosecution charged him with a number of offenses, some of which carried sentencing enhancements based on his gang affiliation.[315] Riley challenged the denial of his motion to suppress this information.[316]

In the second case, Brima Wurie was arrested for selling drugs. While under arrest, police officers noticed that his flip phone was receiving several calls from a number labeled "my house."[317] After searching this cell phone's call log, the officers traced the number to his apartment.[318] The police then went to Wurie's residence and confirmed that it was in fact his home, in part because the woman pictured in his flip phone was found at the apartment.[319] A subsequent search of the apartment revealed drugs and firearms, resulting in multiple federal charges against him.[320] The district court denied his motion to suppress, but the Court of Appeals for the First Circuit reversed and vacated Wurie's three convictions.[321]

309. United States v. Davis, 754 F.3d 1205, 1213 (11th Cir. 2014).
310. *Id.* at 1215.
311. *Id.* at 1217.
312. California v. Riley, 134 S. Ct. 2473 (2014).
313. *Id.* at 2480.
314. *Id.*
315. *Id.* at 2481.
316. *Id.*
317. *Id.*
318. *Id.*
319. *Id.*
320. *Id.*
321. *Id.* at 2482.

In analyzing these two cases, the Court first discussed the history of Fourth Amendment in the context of searches incident to arrest, and ultimately held "that officers must generally secure a warrant before conducting such a search" of a cell phone.[322] The Court continued its analysis by noting that "[d]igital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee's escape. Once an officer has secured a phone and eliminated any potential physical threats, however, data on the phone can endanger no one."[323]

The Court focused next on privacy concerns raised by cell phones, explaining that these devices were essentially small computers that stored immense amounts of data and information.[324] The opinion focused on several reasons that cell phones implicate significant privacy concerns:

> First, a cell phone collects in one place many types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier. A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all of his communications with Mr. Jones for the past several months, as would routinely be kept on a phone.[325]

Finally, the Court emphasized the pervasiveness of cell phones and the fact that people carry them, with all their sensitive information, with them all of the time.[326] Thus, all nine justices held that police must get a search warrant prior to searching a seized cell phone.[327]

C. People Have a Reasonable Expectation of Privacy in Their Cell Phones, Including the Numbers They Dial

While *Katz* established the principle of an individual's reasonable expectation of privacy, *Smith v. Maryland* and *United States v. Miller*[328] are the Supreme Court decisions that are relied upon for the third-party doctrine, which in some ways undercuts *Katz*. In *Miller*, federal agents served grand jury subpoenas issued by the United States Attorney on the

322. *Id.* at 2485.
323. *Id.*
324. *Id.* at 2489.
325. *Id.*
326. *Id.* at 2490.
327. *Id.* at 2495.
328. 425 U.S. 435 (1976).

defendant's banks seeking records to support a criminal investigation.[329] In a motion to suppress, the defendant challenged the subpoenas because they were not issued by a court.[330] Because the defendant had provided his information to the bank in the regular course of his various banking transactions, the Supreme Court determined that he no longer had a reasonable expectation of privacy.[331] Consequently, the Court held "that there was no intrusion into any area in which respondent had a protected Fourth Amendment interest and that the District Court therefore correctly denied respondent's motion to suppress."[332] Of course, in this day and age of online banking, people may have a different expectation of privacy than they used to.

Generally, there is not much in the way of empirical research regarding people's reasonable expectations of privacy.[333] Moreover, there does not appear to be any research questioning people's reasonable expectations of privacy regarding the telephone numbers that they dial with their cell phones. The limited data reflects that individuals, when surveyed, "overwhelmingly expressed agreement with precedent limiting invasions of communications privacy."[334] In one survey, 63.1% of participants agreed with the decision in *Katz* requiring a warrant to record a phone conversation.[335] That rate went up to 91.7% if the phone in question was the participant's cell phone.[336]

Some scholars have asserted that the Supreme Court's determinations of what constitutes "reasonable expectations of privacy" "are often not in tune with commonly held values."[337] The limited existing quantitative research supports this claim. For example, 85.5% of respondents in one survey disagreed with *United States v. Knott*,[338] in which the Supreme Court upheld the warrantless installation of a tracking device on a vehicle.[339] Similarly, in a poll of Californians, 73 percent "favor a law that required the police to convince a judge that a crime has been committed before obtaining location information from

329. *Id.* at 437.

330. *Id.* at 438–39.

331. *Id.* at 445.

332. *Id.* at 440.

333. *See* Blumenthal et al., *supra* note 293, at 334 ("Little relevant empirical research has been conducted on perceptions of privacy . . . ."); Fradella et al., *supra* note 263, at 338 ("Much more research also needs to be conducted to assess the impact of changes in U.S. surveillance and search and seizure jurisprudence on the privacy rights of citizens.").

334. Fradella et al., *supra* note 263, at 338.

335. *Id.* at 366.

336. *Id.*

337. Christopher Slobogin & Joseph E. Schumacher, *Rating the Intrusiveness of Law Enforcement Searches and Seizures*, 17 LAW & HUM. BEHAV. 183, 198 (1993).

338. 460 U.S. 276 (1983).

339. Fradella et al., *supra* note 263, at 366–67.

the cell phone company."[340] Moreover, in a question based on *United States v. Miller*, 85.4% of those surveyed disagreed with the Court's ruling that there is no reasonable expectation of privacy in one's bank records.[341] These results demonstrate a significant disconnect between the Supreme Court's interpretation of what constitutes a reasonable expectation of privacy in various contexts and individual's actual expectations.

Specifically, several state courts have rejected the applicability of *Miller* pursuant to state constitutions.[342] Similarly, various state courts have rejected the reasoning and ruling in *Smith v. Maryland*.[343] In light of numerous state court decisions addressing pen registers, the government's use of a pen register to obtain authorization for cell site simulators is troubling from the perspective of a reasonable expectation of privacy standard. A number of state courts have concluded, based on state constitutions and statutes, that their citizens have such a privacy expectation and that probable cause and a warrant are necessary for a pen register.[344] Interestingly, these various state court decisions regarding

---

340. JENNIFER KING & CHRIS JAY HOOFNAGLE, RESEARCH REPORT: A SUPERMAJORITY OF CALIFORNIANS SUPPORTS LIMITS ON LAW ENFORCEMENT ACCESS TO CELL LOCATION INFORMATION 8 (2008), *available at* www.ftc.gov/os/comments/mobilevoice/534331-00005.pdf.

341. Fradella et al., *supra* note 263, at 366.

342. *See, e.g.*, State v. McAllister, 875 A.2d 866, 875 (N.J. 2005); State v. Thompson, 810 P.2d 415, 418 (Utah 1991) (the Utah Constitution provides individuals "a right to be secure against unreasonable searches and seizures of their bank statements"); Winfield v. Div. of Pari-Mutuel Wagering, Dep't of Bus. Regulation, 477 So. 2d 544, 548 (Fla. 1985) ("[T]he law in the state of Florida recognizes an individual's legitimate expectation of privacy in financial institution records."); Charnes v. DiGiacomo, 612 P.2d 1117, 1121–22, 1124 (Colo. 1980) (en banc) (distinguishing *Miller* and holding that "[a]n individual has an expectation of privacy in records of his financial transactions held by a bank in Colorado.");; People v. Jackson, 452 N.E.2d 85, 89 (Ill. App. Ct. 1983) ("[W]e reject the idea set out in *Miller* that a citizen waives any legitimate expectation in her financial records when she resorts to the banking system.").

343. *See, e.g.*, Commonwealth v. Melilli, 555 A.2d 1254, 1258 (Pa. 1989) (expressly rejecting *Smith v. Maryland*); Richardson v. State, 865 S.W.2d 944, 951–52, 952 n.6 (Tex. Crim. App. 1993) (rejecting *Smith v. Maryland*).

344. *See, e.g.*, People v. Sporleder, 666 P.2d 135, 144 (Colo. 1983) (en banc) (holding that the Colorado Constitution provides a telephone subscriber with a reasonable expectation of privacy in the numbers dialed such that they cannot be obtained without a search warrant based on probable cause); Shaktman v. State, 553 So. 2d 148, 151–52 (Fla. 1989) ("Because the pen register intrudes upon fundamental privacy interests [based on the Florida Constitution], the state has the burden of demonstrating both that the intrusion is justified by a compelling state interest and that the state has used the least intrusive means in accomplishing its goal."); State v. Rothman, 779 P.2d 1, 7 (Haw. 1989) ("[P]ersons using telephones in the State of Hawaii have a reasonable expectation of privacy, with respect to the telephone numbers they call on their private lines . . . ."); State v. Thompson, 760 P.2d 1162, 1165–67 (Idaho 1988) (a pen register was a search pursuant to the Idaho Constitution and required a warrant); State v. Hunt, 450 A.2d 952, 956–57 (N.J. 1982) (the New Jersey Constitution affords individuals the right to privacy in their toll billing records and, by implication, pen register records); Commonwealth v. Beauford, 475 A.2d 783, 791 (Pa. Super. 1984) (holding that individuals have a reasonable expectation of privacy in the telephone numbers one dials and the Pennsylvania Constitution protects individuals against the installation of pen registers without a demonstration of

privacy rights, pen registers, and one's reasonable expectations of privacy were all decided in the 1980s, before the cell phone became ubiquitous in American life. These expectations have not disappeared as pen registers have grown more sophisticated and most people rely exclusively on their cell phones to communicate with others. For example, in *State v. Branigh*,[345] the Court of Appeals of Idaho concluded that the defendant "had a reasonable expectation of privacy in the telephone log records that the State obtained from Sprint and that the State's acquisition of those logs was subject to the restraints of [the Idaho Constitution]."[346] Moreover, this protection extends to the records documenting the dates, times, and recipients of text messages.[347]

These state court decisions just start to scratch the surface of various jurisdictions' notions of reasonable expectations of privacy regarding these matters. It stands to reason that if various people around the country have a reasonable expectation of privacy in preventing law enforcement officials from obtaining their telephone call records based on standard pen register requests, then these same people would have similar privacy expectations in any pen register request for a cell site simulator.

That so many state courts and legislatures conclude that there is a reasonable expectation of privacy regarding pen registers further supports the position that a cell site simulator would have a similar, if not stronger, expectation of privacy. Coupled with the fact that the pen register at issue in *Smith v. Maryland* was a significantly less technologically advanced version of the pen registers typically sought today, there is a good argument that the day for reassessment of the continued viability of the decision is coming. One need look no further than the recent issues involving massive electronic searches of American citizens by the NSA to know that many people believe this day has arrived. Indeed, while a pen register in the *Smith v. Maryland* era obtained the only outgoing telephone numbers called, a pen register for a cell phone provides much more information today, including the telephone numbers dialed for text messages and phone calls; the date, time, duration of such phone calls and text messages; and the location of the cell phone.[348]

---

probable cause); State v. Gunwall, 720 P.2d 808, 813 (Wash. 1986) (en banc) (holding that the Washington Constitution barred the use of a pen register without a search warrant); *see also* Richardson v. State, 865 S.W.2d 944, 953 (Tex. Crim. App. 1993) (en banc) (holding that a pen register may be a search pursuant to the Texas Constitution).

345. 313 P.3d 732 (Idaho Ct. App. 2013).

346. *Id.* at 738 (discussing *Thompson*, 760 P.2d at 1165).

347. *Id.*

348. Kelly, *supra* note 3.

CONCLUSION

The purpose of this Article is not to reject the use of cell site simulators. Indeed, it is clear that these devices can be effective tools in law enforcement arsenals. For example, the use of a cell site simulator near a prison facility can assist in locating a cell phone used by inmates in furtherance of criminal activity.

Nonetheless, there are significant concerns for the privacy rights and interests of third parties. Regarding the applications for the use of cell site simulators, law enforcement officials should minimize the impact that cell site simulators have on such third parties, including by developing a protocol that explains attempts to minimize the invasion of privacy.[349]

It is clear that an application for a cell site simulator seeks authorization for a device unanticipated by Congress in the pen register statute. "If courts find that the new methods do not fit into the statutory definition, they may follow the lead of those courts who have regarded the new practices as completely unregulated."[350] For law enforcement officials to obtain judicial approval for the use of cell site simulators, they should have to seek authorization pursuant to a search warrant consistent with Rule 41 of the Federal Rules of Criminal Procedure. Alternatively, they can persuade Congress to amend the pen register statute to authorize cell site simulators.

Scholars have long called for Congress to amend the ECPA in order to update it to address the myriad of technological developments in surveillance since 1986.[351] As Susan Freiwald has asserted, "[t]he ECPA, because it permits a substantial amount of surveillance to proceed without the requirement of a warrant, let alone the heightened procedural safeguards that apply to wiretapping, should have been quite vulnerable to constitutional challenges."[352] Congressional reticence to amend may require that the courts handle the matter of safeguarding the public: "the Supreme Court has taken a hands-off approach to technological development, refusing to recognize Fourth Amendment privacy barriers to its use. However, the Court has sometimes been willing to intervene even

---

349. *See* Owsley, *supra* note 15, at 46.

350. Freiwald, *supra* note 93, at 999–1000; *see* Bellia, *supra* note 82, at 1382 ("Because application of the Fourth Amendment is in doubt, the statutory rules for acquisition of communications are all the more important. Those provisions, however, reflect significant gaps and ambiguities.").

351. *See* Bellia, *supra* note 82, at 1458 (noting that Congress "could not have anticipated that technological developments would place so many electronic communications in the hands of third parties" when the ECPA was enacted); Orin Kerr, *A User's Guide to the Stored Communications Act and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (2004) (addressing areas of potential reform); Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L REV. 1557, 1559 (2004) (explaining that the statute "has failed to keep pace with changes in and on the Internet and therefore no longer provides appropriate privacy protections").

352. Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, 4 (2007).

at the risk of dramatically changing Fourth Amendment law."[353] Because the ECPA does not provide a suppression remedy, individuals cannot assert claims for violations of the statute themselves, and the courts become all the more important.[354] Such courts are those presided over by magistrate judges who handle the vast majority of these types of requests at their initial stages. Only if these judges safeguard the Constitution and bring a voice to the countless citizens across the country can the reasonable expectations of so many be protected.

353. Arcila, *supra* note 258, at 49.

354. *See* 18 U.S.C. § 2708 (2013); *see also* Freiwald, *supra* note 352, at 4.

***