

IN THE
COURT OF SPECIAL APPEALS OF MARYLAND

September Term, 2015

No. 1496

STATE OF MARYLAND,
Appellant,

v.

KERRON ANDREWS,
Appellee.

APPEAL FROM THE CIRCUIT COURT FOR BALTIMORE COUNTY
(THE HONORABLE KENDRA AUSBY, MOTIONS JUDGE)

BRIEF OF *AMICI CURIAE* AMERICAN CIVIL LIBERTIES UNION,
AMERICAN CIVIL LIBERTIES UNION OF MARYLAND,
AND ELECTRONIC FRONTIER FOUNDATION

David Rocah
ACLU of Maryland Foundation
3600 Clipper Mill Rd., Ste 350
Baltimore, MD 21211
(410) 889-8555

Counsel for *amici curiae*

Jennifer Lynch
Of Counsel
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333

Nathan Freed Wessler
Of Counsel
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
(212) 549-2500

Table of Contents

Interests of Amici Curiae.....	vi
Introduction	1
Argument	2
I. Use of the Hailstorm Violated the Fourth Amendment	2
A. Hailstorm technology is both invasive and precise and therefore may be used, if at all, only pursuant to a warrant based on probable cause.....	2
B. Even if Baltimore Police had obtained a warrant to use the Hailstorm, use of the device would still raise serious Fourth Amendment concerns.	9
II. The Government’s Application Contained Material Omissions Invalidating Any Purported Judicial Authorization To Use A Hailstorm.	10
Conclusion.....	15

Table of Authorities

Cases

<i>Arizona v. Gant</i> , 556 U.S. 332 (2009).....	9
<i>Berger v. New York</i> , 388 U.S. 41 (1967).....	8
<i>City of Los Angeles v. Patel</i> , 135 S. Ct. 2443 (2015).....	vi
<i>City of Ontario v. Quon</i> , 560 U.S. 746 (2010)	vii
<i>In re Application for an Order Authorizing Disclosure of Location Information for a Specified Wireless Telephone</i> , 849 F. Supp. 2d 526 (D. Md. 2011)	4
<i>In re Application for an Order Authorizing Installation and Use of a Pen Register and Trap and Trace Device</i> , 890 F. Supp. 2d 747 (S.D. Tex. 2012)	15
<i>In re Application for an Order Authorizing Use of a Cellular Telephone Digital Analyzer</i> , 885 F. Supp. 197 (C.D. Cal. 1995)	15
<i>In re Application of the U.S. for an Order Relating to Telephones Used by Suppressed</i> , No. 15 M 0021, 2015 WL 6871289 (N.D. Ill. Nov. 9, 2015)	4, 8, 15
<i>Kyllo v. United States</i> , 533 U.S. 27 (2001)	4, 5, 6
<i>Maryland v. King</i> , 133 S. Ct. 1958 (2013);.....	vii
<i>Riley v. California</i> , 134 S. Ct. 2473 (2014).....	vi, 5, 6, 7
<i>Smith v. Maryland</i> , 442 U.S. 735 (1979).....	4, 10
<i>Stanford v. Texas</i> , 379 U.S. 476 (1965)	9
<i>State v. Earls</i> , 70 A.3d 630 (N.J. 2013).....	7
<i>State v. Tate</i> , 849 N.W.2d 798 (Wis. 2014)	6
<i>Tracey v. State</i> , 152 So.3d 504 (Fla. 2014)	4, 6
<i>United States v. Comprehensive Drug Testing, Inc.</i> , 621 F.3d 1162 (9th Cir. 2010)	12
<i>United States v. Jones</i> , 132 S. Ct. 945 (2012)	vii, 6
<i>United States v. Karo</i> , 468 U.S. 705 (1984).....	5
<i>United States v. Leon</i> , 468 U.S. 897 (1984)	10

<i>United States v. Ramirez</i> , 523 U.S. 65 (1998).....	8
<i>United States v. Rigmaiden</i> , No. CR 08-814-PHX-DGC, 2013 WL 1932800, (D. Ariz. May 8, 2013)	6
<i>Upshur v. State</i> , 208 Md. App. 383 (2012)	4
<i>Yeagy v. State</i> , 63 Md. App. 1 (1985)	12
Statutes and Constitutional Provisions	
47 U.S.C. § 1002	10
47 U.S.C. § 333	8
Md. Code Ann. Crim. Proc. § 1-203.1	11
Md. Code Ann., Cts. & Jud. Proc. § 10-4B-01.....	10, 11
U.S. Const., amend. IV	passim
Other Authorities	
Adam Lynn, <i>Tacoma Police Change How They Seek Permission to Use Cellphone Tracker</i> , News Tribune, Nov. 15, 2014	14
Brad Heath, <i>Police Secretly Track Cellphones to Solve Routine Crimes</i> , USA Today, Aug. 24, 2015	1, 13
Cyrus Farivar, <i>Cities Scramble to Upgrade “Stingray” Tracking As End of 2G Network Looms</i> , Ars Technica, Sept. 1, 2014.....	1
Daehyun Strobel, Seminararbeit, Ruhr-Universität, <i>IMSI Catcher</i> (July 13, 2007)	7
Dep’t of Justice Policy Guidance: Use of Cell-Site Simulator Technology (Sept. 3, 2015).....	passim
Devlin Barrett, <i>Americans’ Cellphones Targeted in Secret U.S. Spy Program</i> , Wall St. J., Nov. 13, 2014	1
Fred Clasen-Kelly, <i>CMPD’s Cellphone Tracking Cracked High-Profile Cases</i> , Charlotte Observer, Nov. 22, 2014	15
Hannes Federrath, Multilateral Security in Communications, <i>Protection in Mobile Communications</i> (1999).....	7
Jennifer Valentino-DeVries, <i>How ‘Stingray’ Devices Work</i> , Wall St. J. (Sept. 21, 2011)	3

Justin Fenton, <i>Judge Threatens Detective with Contempt for Declining to Reveal Cellphone Tracking Methods</i> , Balt. Sun, Nov. 17, 2014	6, 12
Kim Zetter, <i>Feds Admit Stingrays Can Disrupt Cell Service of Bystanders</i> , Wired, Mar. 1, 2015	2
Kim Zetter, <i>Turns Out Police Stingray Spy Tools Can Indeed Record Calls</i> , Wired, Oct. 28, 2015	3
Mem. from Stephen W. Miko, Resource Manager, Anchorage Police Department, to Bart Mauldin, Purchasing Officer, Anchorage Police Department (June 24, 2009)	2
PKI Electronic Intelligence GmbH, <i>GSM Cellular Monitoring Systems</i>	2, 6
Ryan Gallagher, <i>Meet the Machines That Steal Your Phone’s Data</i> , Ars Technica, Sept. 25, 2013	1
Stephanie K. Pell & Christopher Soghoian, <i>Your Secret Stingray’s No Secret Anymore: The Vanishing Government Monopoly Over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy</i> , 28 Harv. J.L. & Tech. 1 (2014)	1
Tr. of Suppression Hr’g, <i>State v. Thomas</i> , No. 2008-CF-3350A (Fla. 2d Cir. Ct. Aug. 23, 2010).....	6
U.S. Dep’t of Homeland Sec., Policy Directive 047-02 (Oct. 19, 2015)	13

Interests of Amici Curiae¹

The American Civil Liberties Union (“ACLU”) is a nationwide, non-profit, non-partisan public interest organization of more than 500,000 members dedicated to defending the civil liberties guaranteed by the Constitution. The ACLU of Maryland, the organization’s affiliate in Maryland, was founded in 1931 to protect and advance civil rights and civil liberties in that state, and currently has approximately 14,000 members. The protection of privacy as guaranteed by the Fourth Amendment is of special concern to both organizations. The ACLU has been at the forefront of numerous state and federal cases addressing the right of privacy, and has filed briefs as direct counsel and *amicus curiae* in cases involving cell phone location tracking in general and cell site simulators in particular.

The Electronic Frontier Foundation (“EFF”) is a member-supported, non-profit civil liberties organization that has worked to protect free speech and privacy rights in the online and digital world for 25 years. With roughly 23,000 active donors and dues-paying members nationwide, EFF represents the interests of technology users in both court cases and broader policy debates surrounding the application of law in the digital age. EFF has filed amicus briefs in numerous cases involving the application of Fourth Amendment principles to emerging technologies. *See, e.g., City of Los Angeles v. Patel*, 135 S. Ct. 2443 (2015); *Riley v. California*, 134 S. Ct. 2473 (2014); *Maryland v. King*, 133 S. Ct.

¹ In accordance with Rule 8-511, the parties to this appeal have consented to the filing of this brief. No party other than *amici* made a monetary or other contribution to the preparation or submission of the brief. No counsel to a party in this case authored this brief in whole or in part.

1958 (2013); *United States v. Jones*, 132 S. Ct. 945 (2012); *City of Ontario v. Quon*, 560 U.S. 746 (2010).

Introduction

This case involves the surreptitious use of a “Hailstorm” cell site simulator, one of a class of cell phone surveillance devices commonly known as “Stingrays.”² These privacy-invasive devices have been employed by law enforcement agencies for years with little to no oversight from legislative bodies or the courts due to an intentional policy of secrecy.³ Cell site simulators can be carried by hand, installed in vehicles, or mounted on aircraft.⁴ The devices masquerade as the cellular tower antennas used by wireless companies such as AT&T and Sprint, and in doing so, force *all* mobile phones within the range of the device that subscribe to the impersonated wireless carrier to emit identifying signals, which can be used to locate not only a particular suspect, but bystanders as well.

In this case, Baltimore Police transmitted signals through the walls of homes in a Baltimore neighborhood to force Defendant’s mobile phone to transmit its unique serial number and, as a result, reveal its location. In defending that conduct before this Court,

²“StingRay” is the name for one cell site simulator model sold by the Harris Corporation. Other models include the “TriggerFish,” “KingFish,” and “Hailstorm.” See Ryan Gallagher, *Meet the Machines That Steal Your Phone’s Data*, *Ars Technica*, Sept. 25, 2013, <http://bit.ly/1mkumNf>. StingRays, Hailstorms, and other models of cell site simulators are also called “IMSI catchers,” in reference to the unique identifier—or international mobile subscriber identity—of wireless devices that they track. Stephanie K. Pell & Christopher Soghoian, *Your Secret Stingray’s No Secret Anymore: The Vanishing Government Monopoly Over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy*, 28 *Harv. J.L. & Tech.* 1, 11 (2014). The Hailstorm is Harris Corporation’s newest model, and is capable of identifying LTE (4G) phones. Cyrus Farivar, *Cities Scramble to Upgrade “Stingray” Tracking As End of 2G Network Looms*, *Ars Technica*, Sept. 1, 2014, <http://bit.ly/1x6QKwY>.

³ See Brad Heath, *Police Secretly Track Cellphones to Solve Routine Crimes*, *USA Today*, Aug. 24, 2015, <http://usat.ly/1LtSLdI>.

⁴Gallagher, *supra* note 2; see also Devlin Barrett, *Americans’ Cellphones Targeted in Secret U.S. Spy Program*, *Wall St. J.*, Nov. 13, 2014, <http://on.wsj.com/1EHIEez>.

the government mischaracterizes how the technology operates, minimizes the constitutional privacy interests at stake, and glosses over its lack of candor when seeking judicial authorization to locate Defendant's cell phone. *Amici* submit this brief to provide publicly available facts about the technology's capabilities in order to inform the Court of Fourth Amendment concerns unique to this technology. *Amici* also explain why the government's Fourth Amendment arguments are wrong as a matter of law and why its lack of candor in its application for a pen register order invalidates the order.

Argument

I. Use of the Hailstorm Violated the Fourth Amendment.

A. Hailstorm technology is both invasive and precise and therefore may be used, if at all, only pursuant to a warrant based on probable cause.

Wireless carriers provide coverage through a network of base stations, also known as "cell sites," that connect cell phones to the telephone network. Like other cell site simulator models, a Hailstorm masquerades as a wireless carrier's base station, prompting all wireless devices within range that use the impersonated wireless carrier to communicate with it. Depending on the particular features of the device and how the operator configures them, cell site simulators can be used to identify nearby phones, to precisely locate them,⁵ and can even block service to devices in the area.⁶ Cell site simulators are commonly used by law enforcement agencies in two ways: to collect the

⁵ See, e.g., Mem. from Stephen W. Miko, Resource Manager, Anchorage Police Department, to Bart Mauldin, Purchasing Officer, Anchorage Police Department (June 24, 2009), <http://bit.ly/1P3dhTd> (describing location accuracy to within 25 feet); PKI Electronic Intelligence GmbH, *GSM Cellular Monitoring Systems*, 12, <http://bit.ly/1OsxaOT> (describing location accuracy to within two meters).

⁶ See Kim Zetter, *Feds Admit Stingrays Can Disrupt Cell Service of Bystanders*, *Wired*, Mar. 1, 2015, <http://bit.ly/1K5Aa76>.

unique electronic serial numbers associated with all phones in a given area, or to locate a particular phone “when the officers know the numbers associated with it but don’t know precisely where it is.”⁷ Some versions of the technology can also obtain metadata about a suspect’s calls and text messages or even the contents of those communications, although there is no evidence that Baltimore Police have employed such capabilities.⁸

Cell site simulators locate phones by *forcing* them to repeatedly transmit their unique identifying electronic serial numbers, and then calculating the signal strength and direction of those transmissions until the target phone is pinpointed. (T3 50-51).⁹ This dynamic is essential to understanding the Fourth Amendment status of cell site simulator technology, yet is elided by the government when it argues, incorrectly, that it is an “unproven assumption that it was the cell site simulator which was sending signals to the cell phone, but . . . in fact, it was the phone which sent signals to the Hailstorm device.” Gov’t Br. 8. To the contrary, as explained by the U.S. Department of Justice and numerous other sources, “[c]ell-site simulators . . . function by transmitting as a cell tower. *In response to the signals emitted by the simulator*, cellular devices in the proximity of the device . . . transmit signals to the simulator.” Dep’t of Justice Policy Guidance: Use of Cell-Site Simulator Technology [hereinafter “DOJ Guidance”] 2 (Sept. 3, 2015), <http://www.justice.gov/opa/file/767321/download> (emphasis added); *accord In re Application of the U.S. for an Order Relating to Telephones Used by Suppressed*, No.

⁷ Jennifer Valentino-DeVries, *How ‘Stingray’ Devices Work*, Wall St. J. (Sept. 21, 2011), <http://on.wsj.com/1D2IWcw>.

⁸ Kim Zetter, *Turns Out Police Stingray Spy Tools Can Indeed Record Calls*, Wired, Oct. 28, 2015, <http://bit.ly/1PRCGQC>.

⁹ Citations to “T3” are to the discovery hearing transcript of June 4, 2015.

15 M 0021, 2015 WL 6871289, at *2 (N.D. Ill. Nov. 9, 2015) (“[T]he device causes or forces cell-phones in an area to send their signals – with all the information contained therein – to the cell-site simulator.”); (T3 53 (“[The Hailstorm] draws the phone to our equipment.”)). In other words, the Hailstorm device used in this case did not passively intercept the signals transmitted between Defendant’s phone and Sprint’s network, but rather forced Defendant’s phone to transmit information to the government that it would not otherwise have transmitted to the government.¹⁰

Accordingly, the “third-party doctrine,” as set out in *Smith v. Maryland*, 442 U.S. 735 (1979), and *Upshur v. State*, 208 Md. App. 383 (2012), is inapposite. Those cases involved law enforcement obtaining information from third-party phone companies that was already in the companies’ possession. Unlike the dialed phone numbers transiting the phone company’s network in *Smith* and the subscriber information held in the phone company’s files in *Upshur*, the location information in this case was obtained by a Baltimore Police Department (BPD) officer directly from Defendant’s phone. When the police seek information by directly interacting with a suspect’s phone, no third party is involved, and the Fourth Amendment warrant requirement applies. Just as the Fourth Amendment regulates police use of a thermal imaging camera to remotely obtain information about heat signatures emanating from a home, *Kyllo v. United States*, 533 U.S. 27, 34 (2001), so too does it regulate use of a Hailstorm to solicit and receive data

¹⁰ Even if the government had used a “passive” interception device, locating and tracking a cell phone would still require a warrant. *See Tracey v. State*, 152 So.3d 504, 526 (Fla. 2014) (real-time cell phone location tracking is Fourth Amendment search); *In re Application for an Order Authorizing Disclosure of Location Information for a Specified Wireless Telephone*, 849 F. Supp. 2d 526, 539–43 (D. Md. 2011) (same).

from a cell phone. Both involve direct collection of information by police, not requests for data already held by a third party.

For the following reasons, use of a cell site simulator constitutes a search within the meaning of the Fourth Amendment. Assuming such searches are ever permissible, *see infra* Part I.B, they at a minimum require a warrant. Indeed, federal law enforcement agencies have recently made clear that, absent exigent or exceptional circumstances, a warrant is required. DOJ Guidance at 3.

First, the devices transmit invisible, probing electronic signals that penetrate walls of Fourth Amendment-protected locations, including homes, offices, and other private spaces occupied by the target and innocent third parties in the area. (T3 49). Cell site simulators force cell phones within those spaces to transmit data to the government that they would not otherwise reveal to the government, and allow agents to determine facts about the phone and its location that would not otherwise be ascertainable without physical entry. By pinpointing suspects and third parties while they are inside constitutionally protected spaces, cell site simulators invade reasonable expectations of privacy. *See Kyllo*, 533 U.S. at 34 (thermal imaging to detect heat from home constituted search); *United States v. Karo*, 468 U.S. 705, 715 (1984) (monitoring of radio-location beeper that was taken into residence constituted search).¹¹

¹¹ Indeed, “nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower.” *Riley v. California*, 134 S. Ct. 2473, 2490 (2014). In this situation, “[t]he [cell site simulator] might disclose, for example, at what hour each night the lady of the house takes her daily sauna and bath—a detail that many would consider ‘intimate.’” *Kyllo*, 533

Second, the devices can pinpoint an individual with extraordinary precision, in some cases “with an accuracy of 2 m[eters].”¹² Just as in this case, in cases across the country law enforcement agents have used cell site simulators to pinpoint suspects’ locations not only in free-standing houses, but even in specific apartments or areas within large apartment complexes. *See, e.g., State v. Tate*, 849 N.W.2d 798, 804 (Wis. 2014); *United States v. Rigmaiden*, No. CR 08-814-PHX-DGC, 2013 WL 1932800, at *15 (D. Ariz. May 8, 2013); Tr. of Suppression Hr’g 14, 17, *State v. Thomas*, No. 2008-CF-3350A (Fla. 2d Cir. Ct. Aug. 23, 2010), *available at* <http://bit.ly/1jYUgUT>. In one Baltimore case, police reportedly used a cell site simulator to determine even that the person carrying the target phone was riding on a particular bus.¹³ Accurate electronic location tracking of this type requires a warrant because it intrudes on reasonable expectations of privacy. *Riley v. California*, 134 S. Ct. 2473, 2490 (2014) (noting Fourth Amendment implications of cell phone location data that can “reconstruct someone’s specific movements down to the minute, not only about town but also within a particular building”); *United States v. Jones*, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring in the judgement) (“[T]he use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.”); *id.* at 955 (Sotomayor, J., concurring); *Tracey*, 152 So.3d at 526 (“[T]he use of [a suspect’s] cell site location information emanating from his cell phone in order to track him in real time was a search within the purview of

U.S. at 38. To protect such intimate details, “the Fourth Amendment draws ‘a firm line at the entrance to the house.’” *Id.* at 39.

¹² *See, e.g.,* PKI Electronic Intelligence, *supra* note 5.

¹³ Justin Fenton, *Judge Threatens Detective with Contempt for Declining to Reveal Cellphone Tracking Methods*, Balt. Sun, Nov. 17, 2014, <http://bsun.md/1uE8k7v>.

the Fourth Amendment for which probable cause was required.”); *State v. Earls*, 70 A.3d 630, 586 (N.J. 2013) (tracking a cell phone “can reveal not just where people go—which doctors, religious services, and stores they visit—but also the people and groups they choose to affiliate with and when they actually do so.”).

Third, cell site simulators search the contents of people’s phones by forcing those phones to transmit their electronic serial number and other identifying information held in electronic storage on the device, as well as the identity of the (legitimate) cell tower to which the phone was most recently connected and other stored data. *See* Stipulation, *United States v. Harrison*, No. 14 Cr. 170 (D. Md. Nov. 7, 2014), ECF No. 32-1 (attached as Ex. A) (“The simulator can also collect radio signals containing the channel and cell-site codes identifying the cell location and geographical sub-sector from which the telephone is transmitting.”). As the Supreme Court held last year, searching the contents of a cell phone requires a warrant. *Riley*, 134 S. Ct. 2473.

Fourth, cell site simulators impact third parties on a significant scale. In particular, they interact with and capture information from innocent bystanders’ phones by impersonating one or more wireless companies’ cell sites and thereby triggering an automatic response from all mobile devices on the same network in the vicinity. DOJ Guidance at 5.¹⁴ This is so even when the government is using a cell site simulator with

¹⁴ *See also, e.g.*, Hannes Federrath, *Multilateral Security in Communications, Protection in Mobile Communications*, 5 (1999), <http://bit.ly/1QHLfwk> (“possible to determine the IMSIs of all users of a radio cell”); Daehyun Strobel, Seminararbeit, Ruhr-Universität, *IMSI Catcher 13* (July 13, 2007), <http://bit.ly/1P3dS7i>. (“An IMSI Catcher masquerades as a Base Station and causes every mobile phone of the simulated network operator within a defined radius to log in.”).

the intent to locate or track a particular suspect; collection of innocent bystanders' phone-identifying data and location information is inevitable and unavoidable using current cell site simulator technology. Thus, when using a Hailstorm the police infringe on the reasonable expectations of privacy of large numbers of innocent non-suspects, amplifying the Fourth Amendment concerns. Although there is a serious question whether dragnet searches of this nature are ever allowed by the Fourth Amendment, *see infra* Part I.B, use of this technology must at least be constrained by a probable cause warrant that mandates minimization of innocent parties' data. *In re Application*, 2015 WL 6871289, at *3–4 (mandating protections for innocent third parties in issuance of cell site simulator warrants); *cf. Berger v. New York*, 388 U.S. 41, 57–59 (1967) (similar protections for wiretaps).

Finally, cell site simulators can, as a side-effect of their normal use, disrupt the ability of phones in the area to make calls. *See* DOJ Guidance at 5. The Harris Corporation, the company that manufactures the Hailstorm, has apparently taken steps to ensure that 911 calls are not disrupted. Barrett, *supra* note 4. However, emergency calls to doctors, psychologists, and family members may be blocked while the Hailstorm is in use nearby. This is invasive in general, raises possible conflicts with federal law, *see* 47 U.S.C. § 333 (prohibiting interference with cellular transmissions), and can have enormous consequences for anyone in an emergency situation trying to make an urgent call for assistance. To avoid effecting an unreasonably invasive or destructive search, *see United States v. Ramirez*, 523 U.S. 65, 71 (1998), use of cell site simulators must be strictly constrained and explicitly authorized by a court.

In light of these factors, use of a cell site simulator is presumptively invalid unless the government obtains a valid warrant based on probable cause. *See Arizona v. Gant*, 556 U.S. 332, 338 (2009) (explaining that searches without a warrant are “*per se* unreasonable”). The government did not obtain a warrant to use a cell site simulator device in this case. In fact, it did not request authorization to use a cell site simulator at all, but misled the court by seemingly applying for an order authorizing installation of a run-of-the-mill pen register device. *See infra* Part II.

B. Even if Baltimore Police had obtained a warrant to use the Hailstorm, use of the device would still raise serious Fourth Amendment concerns.

Even in instances where the government obtains a warrant, cell site simulator use raises serious constitutional concerns due to the dragnet nature of the device’s surveillance and the collateral impacts of the device’s broadcasts on innocent third parties. As discussed above, cell site simulators can collect identifying information about large numbers of innocent bystanders’ phones, send electronic signals through the walls of nearby homes and offices, and interfere with bystanders’ ability to make and receive phone calls. The Fourth Amendment was “the product of [the Framers’] revulsion against” “general warrants” that provided British “customs officials blanket authority to search where they pleased for goods imported in violation of the British tax laws.” *Stanford v. Texas*, 379 U.S. 476, 481–82 (1965). Cell site simulators inevitably interact with and collect data from the phones of innocent third parties as to whom there is no individualized suspicion, let alone probable cause. Authorization for such sweeping surveillance raises the type of concerns that animate the prohibition on general warrants.

See United States v. Leon, 468 U.S. 897, 899 (1984) (“[A] warrant may be so facially deficient—i.e., in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid.”).

II. The Government’s Application Contained Material Omissions Invalidating Any Purported Judicial Authorization To Use A Hailstorm.

In its application seeking authorization to locate Defendant’s cell phone, the government misled the court in requesting what appeared to be a run-of-the-mill pen register order, which contained no mention of a cell site simulator, much less any explanation of how such a device operates, the privacy implications for innocent third parties, or the fact that regular use of the cell site simulator can disrupt phone calls nearby. Because the government never asked the court for permission to operate a Hailstorm and withheld crucial details describing it, the court’s order did not authorize, and could not have authorized, its use.

Traditionally, courts recognized a pen register as a device operated by the phone company that records the numbers dialed by a telephone. *Smith v. Maryland*, 442 U.S. 735, 736 & n.1 (1979). Although pen registers now may also “record[]” other “routing, addressing, or signaling information,” Md. Code Ann., Cts. & Jud. Proc. § 10-4B-01(c)(1), the government here sought a pen register order to authorize use of a “Pen Register . . . and Cellular Tracking Device,” (R.54). Maryland’s pen register statute makes no provision for, or even mention of, a “cellular tracking device.”¹⁵ Md. Code

¹⁵ Under federal law, pen register orders may not be used to obtain location information. *See* 47 U.S.C. § 1002(a)(2). Although the Maryland pen register statute does not include this limiting language, as of October 1, 2014, law enforcement in Maryland must obtain a

Ann., Cts. & Jud. Proc. § 10-4B-01. Without a description from the government of what it meant by “cellular tracking device,” it would have been near-impossible for the issuing judge to know that the government was in fact referring to a Hailstorm. Even more unlikely would have been the court’s independent understanding that, unlike a true pen register, a Hailstorm does not merely “record[],” but broadcasts signals that penetrate the walls of every private home in its vicinity and force responses from bystanders’ phones.

The portion of the government’s application that purportedly sought authorization to use a Hailstorm is vague, brief, and buried in a single paragraph of an 11-page filing:

[The government] shall initiate a signal to determine the location of the subject’s mobile device on the service provider’s network or with such other reference points as may be reasonably available, Global Position System Tracing and Tracking, Mobile Locator tools, R.T.T. (Real Time Tracking Tool), . . . Precision Locations and any and all locations

(R.57–58). There is no explanation of what these “tools” are, how they operate, how they will be used, or that they will intrude into constitutionally protected spaces and impact the privacy of bystanders. Moreover, every other relevant paragraph of the application seeks authorization to enlist the assistance of wireless service providers to obtain information about Defendant’s phone, giving the court no way to know that police actually intended to use their own device that mimics a legitimate cell site and bypasses the service providers altogether. (R.56–63). Indeed, *every* relevant paragraph of the order, including the paragraph that permits location tracking, (R.68), directs the assistance of service providers, and thus does not authorize independent use of a Hailstorm by police.

search warrant before tracking the location of a cell phone. Md. Code Ann. Crim. Proc. § 1-203.1, enacted as S.B. 698, 2014 Md. Laws Ch. 191.

The government's omissions fail its duty of candor to the courts. *See United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1176 (9th Cir. 2010) (en banc) (Kozinski, J. concurring) (“A lack of candor in . . . the warrant application must bear heavily against the government in the calculus of any subsequent motion to return or suppress the seized data.”). When omissions from an application for a court order were “made intentionally or with reckless disregard for accuracy,” and where those omissions were material to the court’s decision to grant the order, the order is deemed invalid and derivative evidence must be suppressed. *Yeagy v. State*, 63 Md. App. 1, 8 (1985). The omissions were both intentional and material here. That BPD’s omission of any description of the intent to use a Hailstorm or its capabilities was intentional is made clear by the non-disclosure agreement signed by the Baltimore Police Commissioner and the State’s Attorney for Baltimore City as early as 2011. Non-Disclosure Agreement (July 13, 2011), <http://bit.ly/1QHLo30>. There, the BPD and the State’s Attorney’s Office agreed that they would “not, in any civil or criminal proceeding, use or provide any information concerning the [cell site simulator] equipment/technology . . . beyond the evidentiary results obtained through the use of the equipment/technology including . . . during pre-trial matters [and] in search warrants and related affidavits” *Id.* ¶ 5. Baltimore Police officers have relied on the agreement to resist answering questions from judges and defense counsel in court,¹⁶ and the government has even apparently concealed

¹⁶ Fenton, *Judge Threatens Detective with Contempt*, *supra* note 13.

from *this* Court when it used a cell site simulator.¹⁷ This policy of concealment demonstrates that omission of information from the application in this case was not isolated negligence. Rather, it was part of an intentional course of conduct in which the BPD used cell site simulators thousands of times “but frequently concealed that fact from suspects, their lawyers and even judges.”¹⁸

The omission was also material. By declining to apprise the court that it intended to use a Hailstorm, what the device is, and how it works, the government prevented the court from exercising its constitutional function of ensuring that searches are not overly intrusive, that the rights of non-suspects are protected, and that all aspects of the search are supported by probable cause and described with particularity. The need for candor and specificity when seeking court authorization to use a cell site simulator has recently been recognized by the federal Departments of Justice and Homeland Security, which require that “applications for the use of a cell-site simulator must include sufficient information to ensure that the courts are aware that the technology may be used.” DOJ Guidance at 5; U.S. Dep’t of Homeland Sec., Policy Directive 047-02, at 6 (Oct. 19, 2015).¹⁹ Had the issuing judge had access to full and accurate information, he likely would have withheld or modified the order, as other fully informed judges have done.

When judges have learned that police departments are seeking to use cell site simulators and have understood the capabilities of those devices, they have limited the

¹⁷ Heath, *Police Secretly Track Cellphones to Solve Routine Crimes*, *supra* note 3 (citing *Redmond v. State*, 213 Md. App. 163 (Md. Ct. Spec. App. 2013)).

¹⁸ *Id.*

¹⁹ Available at <http://1.usa.gov/1mqvY88>.

scope of orders or rejected pen register applications in favor of a warrant standard. In one federal investigation in New Jersey, for example, the government submitted an application for a pen register order to use a cell site simulator that included significantly more detail than was provided in this case, explaining that the device will “mimic[] one of Sprint’s cell towers to get the Target [phone] to connect to it” and “data [will be] incidentally acquired from phones other than the Target.” Appl. for Pen Register Order ¶¶ 3–7, *United States v. Williams*, No. 13 Cr. 548, Mag. No. 12-3092 (D.N.J. July 13, 2012), ECF No. 63-8 (attached as Ex. B). Based on the government’s description, and recognizing that a pen register order cannot authorize electronic surveillance that invades constitutionally protected spaces, the federal magistrate judge reviewing the application modified the government’s proposed order to prohibit the FBI from using the cell site simulator “in any private place or where [FBI agents] have reason to believe the Target [phone] is in a private place.” Order at 5, *id.*

Other judges have similarly imposed reasonable protections when presented with accurate and full information. After a local newspaper investigation in Tacoma, Washington, revealed that police had used a cell site simulator more than 170 times over five years but had concealed their intent to do so from judges when seeking court orders, local judges collectively imposed a requirement that the government spell out whether it is seeking to use a cell site simulator in future applications, and imposed limits on retention of bystanders’ data.²⁰ Similarly, after the local newspaper in Charlotte, North

²⁰ Adam Lynn, *Tacoma Police Change How They Seek Permission to Use Cellphone Tracker*, News Tribune, Nov. 15, 2014, <http://bit.ly/1T4FHeA>.

Carolina, revealed that police had been using cell site simulators for eight years pursuant to pen register orders, but had not made their intent to do so explicit in their applications, a judge denied an application for such an order, a first for that court.²¹ A federal magistrate judge in Illinois recently issued an opinion explaining the importance of courts having full and accurate information about cell site simulator use, and mandating that future cell site simulator warrants require police to minimize collection and retention of bystanders' data. *In re Application*, 2015 WL 6871289.

Here, had the government told Judge Williams it intended to use a Hailstorm and described the device and its impact on bystanders, he could have denied the application, imposed limits on use of the device, or directed the government to apply for a warrant instead. Federal judges have responded to pen register applications to use a cell site simulator along these lines. *In re Application for an Order Authorizing Installation and Use of a Pen Register and Trap and Trace Device*, 890 F. Supp. 2d 747 (S.D. Tex. 2012); *In re Application for an Order Authorizing Use of a Cellular Telephone Digital Analyzer*, 885 F. Supp. 197, 201 (C.D. Cal. 1995). The government's intentional omission of material information requires suppression, both because it invalidates the order, and because, even if the order were valid on its own terms, such order simply did not and could not authorize conduct that the government did not present for approval.

Conclusion

Amici respectfully urge this Court to affirm the trial court's suppression ruling.

²¹ Fred Clasen-Kelly, *CMPD's Cellphone Tracking Cracked High-Profile Cases*, Charlotte Observer, Nov. 22, 2014, <http://bit.ly/1Qj5cvb>.

Dated: December 22, 2015

Respectfully Submitted,



David Rocah
ACLU of Maryland Foundation
3600 Clipper Mill Rd., Ste 350
Baltimore, MD 21211
(410) 889-8555

Counsel for *amici curiae*

Nathan Freed Wessler
Of Counsel
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
(212) 549-2500

Jennifer Lynch
Of Counsel
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333

Statement of Type Style and Point Size

This brief complies with the requirements of Rules 8-112 and 8-504, and is prepared in Times New Roman, 13-point font.

Certificate of Service

I hereby certify that on this 22nd of December 2015, I caused to be mailed first class, postage prepaid, two copies of the foregoing brief to:

Robert Taylor, Jr.
Assistant Attorney General
Office of the Attorney General
Criminal Appeals Division
200 Saint Paul Place
Baltimore, MD 21202

Counsel for Appellant

Daniel Kobrin
Office of the Public Defender
Maryland Office of the Public Defender
Appellate Division
6 St. Paul Street, Suite 1302
Baltimore, MD 21202

Counsel for Appellee



David Rocah

EXHIBITS

- **Exhibit A**

- Stipulation, *United States v. Harrison*, No. 14 Cr. 170 (D. Md. Nov. 7, 2014), ECF No. 32-1

- **Exhibit B**

- Appl. for Pen Register Order, *United States v. Williams*, No. 13 Cr. 548, Mag. No. 12-3092 (D.N.J. July 13, 2012), ECF No. 63-8

EXHIBIT A

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND**

UNITED STATES OF AMERICA

v.

ROBERT HARRISON

Defendant.

*
*
*
*
*
*
*
*
*

CRIMINAL NO. 1:14-CR-00170-CCB

**RESPONSE BY THE UNITED STATES OF AMERICA
TO HARRISON'S MOTION TO COMPEL**

Now comes the United States of America by its attorneys, Rod J. Rosenstein, United States Attorney for the District of Maryland James Warwick, Assistant United States Attorney; and Anthony J. Enright, Special Assistant United States Attorney, and responds in opposition to Defendant Robert Harrison's Motion to Compel Disclosure of Evidence Related to the Government's Use of a Cell Site Simulator (hereinafter "Mot"). Harrison has moved to suppress evidence resulting from the Government's use of a cell-site simulator during the investigation of Harrison (Dkt. # 29), and seeks the production of additional documents about the simulator and the identities of officers who operated it. Harrison is not entitled to any additional information and, accordingly, the Government respectfully requests that this Court deny his Motion.

I. BACKGROUND

A. *The Investigation of Harrison*

In early 2014, law-enforcement agents were investigating the involvement of Derrick Smith in a murder-for-hire conspiracy. Sources had stated to law enforcement that Smith had, on

September 28, 2008, worked with others to kill an individual named Kevin Rouser and that Smith had recently been hired to commit another murder.

Law-enforcement agents purchased a phone for purposes of this investigation (hereinafter the "Subject Phone") in early 2014. Through confidential sources, agents learned that several calls involving both Smith and Harrison were placed to and from the Subject Phone coordinating the murder for hire. On February 4, 2014 an undercover police officer gave the Subject Phone to Smith.

On the day after agents gave the Subject Phone to Smith, February 5, agents obtained an Order from the Baltimore City Circuit Court permitting them to wirelessly track for 60 days the Subject Phone. The Order, which is attached as Exhibit 1 to Harrison's Motion to Suppress, explicitly authorizes use of a "Cellular Tracking Device." (Harrison Motion to Suppress Exhibit 1, at 12.) It also authorizes the use of a "Pen Register," which is a term defined under Maryland law as a "device or process that records and decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted." Md. Code, Cts. & Jud. Proc. § 10-4B-01(c)(1). The Order further authorizes use of a "Trap & Trace," which is defined under Maryland Law as a "device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication." *Id.* § 10-4B-01(d)(1). Additionally, the Order explicitly permits government to "initiate a signal to determine the location of the subject's mobile device," to obtain precision location information, and to "employ surreptitious or duplication of facilities, technical devices or equipment." (Harrison Motion to Suppress

Exhibit 1, at 12-13.) The Order was based on a finding of probable cause, and was signed by Judge Barry G. Williams of the Baltimore City Circuit Court (*Id.* at 11, 17.)

In late March of 2014, law-enforcement officers used a cell-site simulator to assist them in identifying the location of the phone. The cell-site simulator is a device that can transmit to a cell phone a radio signal to which the phone will respond by registering its mobile identification number and its electronic serial number, which is a number assigned by the phone's manufacturer and programmed into the telephone. The cell-site simulator can only interact with the cell-phone when the cell-phone is turned on. The simulator can also collect radio signals containing the channel and cell-site codes identifying the cell location and geographical sub-sector from which the telephone is transmitting. The mobile identification number, electronic serial number, channel codes, and cell-site codes are transmitted continuously as a necessary component of cellular telephone call direction and processing. This information is not dialed or otherwise controlled by the cellular-telephone user. Instead, the transmission of the telephone's electronic serial number and mobile identification number to the nearest cell site occurs automatically when the cellular telephone is turned on. This automatic registration with the nearest cell site is the means by which the cellular service provider ordinarily connects with and identifies the account, determines where to send calls, and reports constantly to the customer's telephone information regarding signal power, status, and mode.

Law enforcement agents initially determined that the phone was located somewhere within the multi-dwelling structure at 3805 Chatham Road in Baltimore City. Agents knocked on the door to the third floor apartment at that location, and Harrison answered and invited them into the apartment where they recognized, and later seized, the Subject Phone.

B. Discovery

In April of 2014, after Harrison was indicted, the Government and Harrison entered into a written agreement stating the terms under which the government would provide discovery in this case. Consistent with its obligations under applicable law, the Government has provided discovery to Harrison in accordance with the terms of this agreement. That discovery has included items sought by Harrison's motion to compel, such as reports of the investigation of Harrison that are within the Government's possession, custody, and control.

Additionally, the Government has attached as Exhibit 1 to this response a stipulation of facts about the government's use of a cell-site simulator. The stipulation identifies facts sufficient to enable the Court to resolve Harrison's Motion to Suppress.

II. DISCUSSION

To the extent Harrison's Motion to Compel seeks information beyond what the Government has already produced, it is without merit for at least two reasons. First, the Government has already produced discovery as required under applicable law, and Harrison has not identified any basis for obtaining the additional discovery that he seeks. Second, the additional information that Harrison seeks is protected from discovery by the qualified privilege for sensitive law-enforcement techniques, and Harrison has failed to meet the standard for overcoming that privilege. Each of these reasons is addressed in turn.

First, Harrison has not identified any basis for obtaining additional discovery. The obligation of the Government to provide a criminal defendant with discovery is ordinarily limited to the extent required by "a statute, rule of criminal procedure, or some other entitlement." *United States v. Uzenski*, 434 F.3d 690, 709 ("Generally, criminal defendants do not have a constitutional right to discovery, absent a statute, rule of criminal procedure, or some

other entitlement.”). Nothing about the information that Harrison seeks suggests that it is discoverable under the Jencks Act, 28 U.S.C. § 3500, *Brady v. Maryland*, 373 U.S. 83 (1963), or *Giglio v. United States*, 405 U.S. 150 (1972). And the government has already produced materials under Rule 16. Harrison does not cite any authority for the additional discovery he requests, but presumably he seeks to invoke Rule 16(a)(1)(E)(i), which permits discovery of items “material to preparing the defense.” (See Mot. 3 (seeking “access to information that is material to various suppression issues.”)).

Rule 16(a)(1)(E)(i) does not entitle Harrison broadly to “information”; instead it is limited to “documents and objects” material to preparing the defense that are “within the government’s possession, custody, or control.” Fed. R. Crim. P. 16(a)(1)(E). The Rule does not entitle Harrison to information not contained in documents that already exist, such as the “[t]he identities of the officers or other personnel” that he requests. (Mot. 4.) *See United States v. Rigmaiden*, 844 F. Supp. 2d 982, 997 (D. Ariz. 2012) (Rule 16(a)(1)(E)(i) “does not require the government to create documents that may provide information a defendant desires to obtain, nor does it require the government to present agents or witnesses for interviews or in-court examination.”).

Harrison has not made the “prima facie showing of materiality” required to prevail on a motion to compel discovery under Rule 16(a)(1)(E). 2 Charles Alan Wright et al., *Federal Practice & Procedure* § 254 (4th ed.). To make that showing, “there must be some indication that the pretrial disclosure of the disputed evidence would . . . enable[] the defendant significantly to alter the quantum of proof in his favor.” *United States v. Caro*, 597 F.3d 608, 621 (4th Cir. 2010) (quotation marks omitted) (quoting *United States v. Ross*, 511 F.2d 757, 763 (5th Cir. 1975)). Harrison notes that, in his motion to suppress, he “argues that use of the device

amounted to searches of his home, cell phone, and person” and offers the conclusion that “[t]he details of how the cell site simulator was used, and how it works, are necessary to determine whether the officers’ conduct was unlawful.” (Mot. 4-5.) Harrison’s Motion, however, contains no explanation of how the evidence he seeks would significantly “alter the quantum of proof” beyond the discovery that he has already received and the Government’s stipulation, and his conclusion to the contrary offers him no support. *Caro*, 597 F.3d 608, 621-22 (4th Cir. 2010) (“Neither a general description of the information sought nor conclusory allegations of materiality suffice” (quotation marks omitted) (quoting *United States v. Mandel*, 914 F.2d 1215, 1219 (9th Cir. 1990))). On that basis, Harrison’s Motion to Compel should be denied.

Second, to the extent Harrison’s Motion seeks additional information about the Government’s use of a cell-site simulator that otherwise would be discoverable, this Court should reject Harrison’s Motion on the basis of the privilege applicable to information about sensitive law-enforcement techniques. Courts have applied this privilege to limit discovery and testimony about information that could enable criminals to frustrate future government investigations and potentially jeopardize the security of ongoing investigations. *See United States v. Cintolo*, 818 F.2d 980, 1002 (1st Cir. 1987). The privilege is qualified, but a defendant can overcome it only by showing that he “needs the evidence to conduct his defense and that there are no adequate alternative means of getting at the same point.” *Id.*

The information that Harrison seeks is subject to the privilege for sensitive law-enforcement techniques. Courts have found information that could limit the effectiveness of future investigations or jeopardize the security of ongoing investigations to be subject to the privilege in a number of different contexts. For example, the Supreme Court has recognized a privilege to withhold the identity of government informants. *Roviaro v. United States*, 353 U.S.

53,59-60 (1957). And courts have held the privilege applicable to information about the location of a police surveillance post, *United States v. Harley*, 682 F.2d 1018, 1020 (D.C. Cir. 1982), and about “the nature and location of electronic surveillance equipment,” *United States v. Van Horn*, 789 F.2d 1492, 1507 (11th Cir. 1986); *accord Cintolo*, 818 F.2d at 1002.

What Harrison requests, “[t]he details of how the cell-site simulator was used, and how it works,” (Mot. 4) falls squarely within the scope of the privilege. As one court recently explained in the context of holding the privilege applicable to information about a cell-site simulator used in another investigation, “the precise technology used . . . and the precise manner in which it was used, if disclosed, would educate the public and adversaries of law enforcement on how precisely to defeat [law-enforcement] surveillance efforts.” *United States v. Rigmaiden*, 844 F. Supp. 2d 982, 994 (D. Ariz. 2012). Similarly, the *Rigmaiden* court explained, “[d]isclosures of the specific identities of agents involved in this operation could jeopardize their safety and would effectively eliminate them as law-enforcement assets used in electronic surveillance.” *Id.* The same concerns attend the information that Harrison seeks about the government’s use of a cell-site simulator in this case. Accordingly, the information is subject to the privilege for sensitive law-enforcement techniques and is not subject to discovery absent a sufficient showing of necessity by Harrison. *See id.*; *Cintolo*, 818 F.2d at 1002.

Harrison has not shown that he “needs the evidence to conduct his defense and that there are no adequate alternative means of getting at the same point,” as required to overcome the privilege. *United States v. Cintolo*, 818 F.2d 980, 1002 (1st Cir. 1987). Harrison has already filed a detailed motion to suppress that cites a host of public information and argues that the Government’s use of a cell-site simulator constituted a search — under both a trespass and reasonable expectation of privacy theory — of Harrison’s home, phone, and even his person, and

that the search was conducted without a warrant. (*See generally* Motion to Suppress.) Harrison can make all of the points that he has raised based on information described in his Motion to Suppress and materials already produced by the Government. Harrison's Motion to Compel contains no showing of greater need; it contains little more than a brief summary of his Motion to Suppress and conclusory statements that the "details" he requests are "necessary to determine whether the officers' conduct was unlawful" and that "Harrison has no alternative means of learning how the technology was used in the investigation leading to his arrest." (Mot. 4-5.)

III. CONCLUSION

Because no basis exists for requiring the Government to provide the additional discovery sought by Harrison and the information he seeks is subject to the privilege for sensitive law-enforcement techniques, the Government respectfully requests that this Court deny Harrison's motion to compel.

Respectfully submitted,

Rod J. Rosenstein
United States Attorney

/s/ _____
Anthony J. Enright
Special Assistant United States Attorney
36 S. Charles Street
Fourth floor
Baltimore, Maryland 21201
(410) 209-4800

/s/ _____
James G. Warwick
Assistant United States Attorney
36 S. Charles Street
Fourth floor
Baltimore, Maryland 21201
(410) 209-4800

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND**

UNITED STATES OF AMERICA

v.

ROBERT HARRISON

Defendant.

*
*
*
*
*
*
*
*
*
*

CRIMINAL NO. 1:14-CR-00170-CCB

STIPULATION

Now comes the United States of America by its attorneys, Rod J. Rosenstein, United States Attorney for the District of Maryland James Warwick, Assistant United States Attorney; and Anthony J. Enright, Special Assistant United States Attorney, and stipulates to the following facts for purposes of Defendant Robert Harrison’s October 10, 2014 Motion to Suppress Evidence Resulting from Use of Cell Site Simultaor.

The cell-site simulator used during the investigation in this case is a device that can transmit to a cell phone a radio signal to which the phone will respond by registering its mobile identification number and its electronic serial number, which is a number assigned by the phone’s manufacturer and programmed into the telephone. The cell-site simulator can only interact with the cell-phone when the cell-phone is turned on. The simulator can also collect radio signals containing the channel and cell-site codes identifying the cell location and geographical sub-sector from which the telephone is transmitting. The mobile identification number, electronic serial number, channel codes, and cell-site codes are transmitted continuously as a necessary component of cellular telephone call direction and processing. This information is

not dialed or otherwise controlled by the cellular-telephone user. Instead, the transmission of the telephone's electronic serial number and mobile identification number to the nearest cell site occurs automatically when the cellular telephone is turned on. This automatic registration with the nearest cell site is the means by which the cellular service provider ordinarily connects with and identifies the account, determines where to send calls, and reports constantly to the customer's telephone information regarding signal power, status, and mode.

EXHIBIT B

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

ORIGINAL FILED

IN THE MATTER OF THE :
APPLICATION OF THE UNITED :
STATES OF AMERICA FOR AN ORDER : **ORDER**
AUTHORIZING THE INSTALLATION :
AND USE OF PEN REGISTER AND : Hon. Patty Shwartz
TRAP AND TRACE DEVICES FOR THE :
CELLULAR TELEPHONE FACILITY : Mag. No. 12-3092
ASSIGNED TELEPHONE NUMBER 908- :
448-3855 : (UNDER SEAL)

JUL 15 2014

PATTY SHWARTZ
U.S. MAG. JUDGE

THIS MATTER having come before the Court upon an application under Title 18, United States Code, Sections 2703(d) and 3122, by Paul J. Fishman, United States Attorney for the District of New Jersey (by Osmar J. Benvenuto, Assistant United States Attorney) seeking an order (a) authorizing the installation and use of pen register and trap and trace devices under Title 18, United States Code, Section 3122 et seq.; (b) requiring the disclosure of records and other information under Title 18, United States Code, Section 2703, and the All Writs Act, 28 United States Code, Section 1651; and (c) authorizing the Federal Bureau of Investigation to deploy mobile pen register and trap and trace equipment to determine the general location of the cellular telephone facility assigned telephone number 908-448-3855, which is issued by Sprint-Nextel ("Sprint") including any other telephones or telephone numbers accessed by equipment using the same unique hardware (e.g., IMEI/ESN/MEID/MAC) or unique subscriber identity (e.g., MDN/MSID/MIN/IMSI/UFMI) (as those terms are defined below¹), and any other

¹ Cell phone service providers use a variety of numbers to identify phone handsets used on their respective systems, including, for hardware, the International Mobile Equipment Identity ("IMEI"), Electronic Serial Number ("ESN"), Mobile Equipment Identity ("MEID") and Media Access Control ("MAC") Address; or, for subscriber identity, Mobile Directory Number

telephones assigned to the same telephone number (“the Target Facility”); and the applicant having certified that the information likely to be obtained by the installation and use of pen register and trap and trace devices is relevant to an ongoing criminal investigation concerning the Specified Federal Offenses identified in the application by subjects identified in that application and others known and unknown; and

IT APPEARING that information likely to be obtained from the pen register and trap and trace devices, including caller identification, is relevant to the ongoing criminal investigation; and

IT FURTHER APPEARING that there are specific and articulable facts showing that and there are reasonable grounds to believe that real-time location information concerning the Target Facility (including all cell site location and registration information but not including GPS, E-911, or other precise location information) and information about subscriber identity, including the name, address, local and long distance telephone connection records, length of service (including start date) and types of service utilized, telephone or instrument number or other subscriber number or identity, and means and source of payment for such service (including any credit card or bank account number), for all subscribers to all telephone numbers, published and non-published, derived from the pen register and trap and trace devices, are relevant and

(“MDN”), Mobile Station Identity (“MSID”), Mobile Identification Number (“MIN”) or Universal Fleet Member Identifier (“UFMI”, for Nextel’s “Direct Connect”). IMEI and IMSI are terms associated with specific technologies, including GSM, iDEN and UMTS; while ESN, MEID and MSID/MIN are terms associated with CDMA and older technologies. In every case, the equipment manufacturer or the communications provider assigns a unique value to each device/customer. Applicability to traceable hardware or subscriber changes has become a long-standing cornerstone to intercept orders, necessary to defeat “SIM-swapping” and other techniques increasingly used to thwart law enforcement investigations.

material to the ongoing criminal investigation;

IT IS on this ___ day of July, 2012,

ORDERED, under Title 18, United States Code, Section 3123, that agents of the Federal Bureau of Investigation are authorized to install and use pen register and trap and trace devices without knowledge of, or notification to, the subscriber, to record and decode dialing, routing, addressing, and signaling information transmitted from the Target Facility, including telephone numbers dialed and pulsed, the date and time of dialings and pulsings, and the length of time the telephone receiver in question is off the hook; and to capture the incoming electronic and other impulses that identify the originating number and other dialing, routing, addressing, and signaling information reasonably likely to identify the source of wire communications to the Target Facility, including caller identification, whenever such electronic and other impulses are sent from or to any location within the jurisdiction of the United States, for the telephones and telephone numbers from which calls are placed to the Target Facility, the date and time of dialings and pulsings, and the length of time the telephone receiver in question is off the hook, for incoming and outgoing calls for a period of 60 days; and it is further

ORDERED, under Title 18, United States Code, Section 3123(b)(2), that Sprint, a provider of electronic communication service, furnish agents of the Federal Bureau of Investigation all information, facilities, and technical assistance necessary to accomplish the installation and use of pen register and trap and trace devices unobtrusively and with minimum interference to the service currently accorded persons whose dialings or pulsings are the subject of the pen register and trap and trace devices; including the make and model of the handset that is associated with or assigned to the Target Facility; and it is further

ORDERED that, in accordance with Title 18, United States Code, Section 3121(c), the Federal Bureau of Investigation will use the technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to dialing, routing, addressing, and signaling information utilized in the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communication; and it is further

ORDERED, under Title 18, United States Code, Section 2703(d), that Sprint furnish expeditiously real-time location information concerning the Target Facility (including all cell site location information but not including GPS, E-911, or other precise location information) for a period of 60 days from the date of this Order; and it is further

ORDERED, under Title 18, United States Code, Section 2703(d), that AT&T, T-Mobile U.S.A., Inc., Verizon Wireless, Metro PCS, Sprint-Nextel and any and all other providers of electronic communication service shall, not later than five business days from the receipt of a request from the Federal Bureau of Investigation furnish all information about subscriber identity, including the name, address, local and long distance telephone connection records, length of service (including start date) and types of service utilized, telephone or instrument number or other subscriber number or identity, and means and source of payment for such service (including any credit card or bank account number), for all subscribers to all telephone numbers, published and non-published, derived from the pen register and trap and trace devices for a period of 60 days from the date of this Order; and it is further

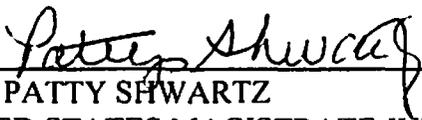
ORDERED, under Title 18, United States Code, Section 3123, that agents of the Federal Bureau of Investigation are authorized to deploy mobile pen register equipment to

monitor the dialing, routing, addressing, and signaling information of the Target Facility in order to determine its general location for a period of 14 consecutive days beginning no later 10 days from the date of this Order, but in no event to use the mobile equipment, absent other authority, ^{use the equipment to} 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;~~ ^{many private place or where they have reason to believe the Target Facility is in a private place}

ORDERED that Sprint be compensated by the Federal Bureau of Investigation for reasonable expenses incurred in providing information, facilities, and technical assistance for the pen register and trap and trace devices; and it is further

ORDERED, under Title 18, United States Code, Section 3123(d), that the Service Providers and their agents, employees, and representatives shall not disclose to any person the existence of this Order, the application upon which it is based, the pen register and trap and trace devices, the disclosure of records, or the investigation unless otherwise ordered by the Court; and it is further

ORDERED that, with the exception of copies of this Order necessary for its implementation, this Order, the application upon which it is based, and all other papers related to this application are sealed until otherwise ordered by the Court.


HON. PATTY SHWARTZ
UNITED STATES MAGISTRATE JUDGE

**UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY**

IN THE MATTER OF THE :
APPLICATION OF THE UNITED :
STATES OF AMERICA FOR AN ORDER : **SEALED APPLICATION**
AUTHORIZING THE INSTALLATION :
AND USE OF PEN REGISTER AND : Hon. Patty Shwartz
TRAP AND TRACE DEVICES FOR THE :
CELLULAR TELEPHONE FACILITY : Mag. No. 12-3092
ASSIGNED TELEPHONE NUMBER :
908-448-3855 :

The United States of America (Paul J. Fishman, United States Attorney for the District of New Jersey, by Osmar J. Benvenuto, Assistant United States Attorney), hereby applies to the Court for an order (a) authorizing the installation and use of a pen register and trap and trace device under Title 18, United States Code, Section 3122 et seq.; (b) requiring the disclosure of records and other information under Title 18, United States Code, Section 2703, and the All Writs Act, 28 United States Code § 1651; and (c) authorizing the Federal Bureau of Investigation to deploy mobile pen register and trap and trace equipment to determine the general location of the cellular telephone facility assigned telephone number 908-448-3855, which is issued by Sprint-Nextel (“Sprint”), including any other telephones or telephone numbers accessed by equipment using the same unique hardware (e.g., IMEI/ESN/MEID/MAC) or unique subscriber identity (e.g., MDN/MSID/MIN/IMSI/UFMI) (as those terms are defined below¹), and any other

¹ Cell phone service providers use a variety of numbers to identify phone handsets used on their respective systems, including, for hardware, the International Mobile Equipment Identity (“IMEI”), Electronic Serial Number (“ESN”), Mobile Equipment Identity (“MEID”) and Media Access Control (“MAC”) Address; or, for subscriber identity, Mobile Directory Number (“MDN”), Mobile Station Identity (“MSID”), Mobile Identification Number (“MIN”) or Universal Fleet Member Identifier (“UFMI”, for Nextel’s “Direct Connect”). IMEI and IMSI are terms associated with specific technologies, including GSM, iDEN and UMTS; while ESN, MEID and MSID/MIN are terms associated with CDMA and older technologies. In every case,

telephones assigned to the same telephone number (“the Target Facility”). This application is based upon the following facts:

1. I am an “attorney for the Government” as defined in Rule 1(b)(1) of the Federal Rules of Criminal Procedure, and therefore I may apply for an order (a) authorizing the installation and use of a pen register and trap and trace device under Title 18, United States Code, Section 3122, and (b) requiring the disclosure of records and other information under Title 18, United States Code, Section 2703.

2. I certify that:

a. Special Agents of the FBI are engaged in an investigation in New Jersey involving seven armed bank robberies: on September 26, 2011 at the Financial Resources Federal Credit Union in Franklin Township, New Jersey; on November 21, 2011 at Somerset Savings Bank in Somerville, New Jersey; on February 27, 2012 at Provident Bank in Piscataway, New Jersey; on April 17, 2012 at Provident Bank in Clifton, New Jersey; on May 22, 2012 at Provident Bank in Piscataway, New Jersey; on June 20, 2012, at approximately 11:18 a.m., Fulton Bank, located at 700 Middlesex Avenue, Metuchen, New Jersey; on July 12, 2012, at Unity Bank, located at 1230 Bound Brook Road, Middlesex, New Jersey. In violation of 18 U.S.C. § 2113(a), the perpetrators did take or attempt to take from the persons and presence of the employees of those banks, money belonging to and in the care, custody, control, management

the equipment manufacturer or the communications provider assigns a unique value to each device/customer. Applicability to traceable hardware or subscriber changes has become a long-standing cornerstone to intercept orders, necessary to defeat “SIM-swapping” and other techniques increasingly used to thwart law enforcement investigations.

and possession of the bank, a financial institution whose deposits were then insured by the Federal Deposit Insurance Corporation;

b. information likely to be obtained from the pen register and trap and trace devices, including caller identification, is relevant to the ongoing criminal investigation;

i. On September 26, 2011, at approximately 9:46 a.m., Financial Resources Federal Credit Union, which is located at 780 Easton Avenue, Franklin Township, New Jersey, was robbed by a male armed with a handgun and wearing a bandana, a hooded sweat shirt, and white gloves. Shortly before the robbery commenced, a female, who is believed to have been working in concert with the robber, entered the bank, apparently as part of an effort to surveil it prior to the robbery. Following the robbery, the robber was seen outside the bank entering the passenger side of a vehicle. The loss sustained was approximately \$20,339.00.

ii. On November 21, 2011, at approximately 9:49 a.m., Somerset Savings Bank, which is located at 64 West End Avenue, Somerville, New Jersey, was robbed by a male armed with a handgun and wearing a bandana, a hooded sweat shirt, and white gloves. Shortly before the robbery commenced, a female, who is believed to have been working in concert with the robber, entered the bank, apparently as part of an effort to surveil it prior to the robbery. The loss sustained was approximately \$14,691.00.

iii. On February 27, 2012, at approximately 9:30 a.m., Provident Bank, located at 100 Shelton Road, Piscataway, New Jersey, was robbed by a male armed with a handgun and wearing a bandana, a hooded sweat shirt, and white gloves. Shortly before the robbery commenced, a male, who is believed to have been working in concert with the

robber, entered the bank, apparently as part of an effort to surveil it prior to the robbery. The loss sustained was approximately \$43,963.00.

iv. On April 17, 2012, at approximately 11:00 a.m., Provident Bank, located at 562 Lexington Avenue, Clifton, New Jersey, was robbed by a male armed with a handgun and wearing a bandana, a hooded sweat shirt, and white gloves. Following the robbery, the robber was seen outside the bank entering the passenger side of a vehicle. The loss sustained was approximately \$10,093.00.

v. On May 22, 2012, at approximately 9:46 a.m., Provident Bank, located at 100 Shelton Road, Piscataway, New Jersey, was robbed by a male armed with a handgun and wearing a bandana, a hooded sweat shirt, and white gloves. The loss sustained was approximately \$13,398.00.

vi. On June 20, 2012, at approximately 11:18 a.m., Fulton Bank, located at 700 Middlesex Avenue, Metuchen, New Jersey, was robbed by a male armed with a handgun and wearing a bandana, a hooded sweat shirt, and white gloves. Shortly before the robbery commenced, a female, who is believed to have been working in concert with the robber, entered the vestibule of the bank, apparently as part of an effort to surveil it prior to the robbery. The loss sustained was approximately \$7,000.

vii. On July 12, 2012, at approximately 11:50 a.m., Unity Bank, located at 1230 Bound Brook Road, Middlesex, New Jersey, was robbed by a male armed with a handgun and wearing a bandana, a hooded sweat shirt, and white gloves (the "July 12 Robbery). Prior to the robbery, a female, who is believed to have been working in concert with

the robber, entered the bank, apparently as part of an effort to surveil it prior to the robbery. The loss sustained was approximately \$9,000.

viii. There is more than one individual involved in the aforementioned bank robberies. There is a high probability that these individuals utilized, during the time period covered by this Application, cellular telephones in the furtherance of their criminal activity, and/or to report to other persons the fruits of their criminal activity.

ix. Shortly before the July 12 Robbery, an unarmed off-duty police officer (the "Officer") parked across from the Unity Bank observed a male armed with a handgun and wearing a face covering, a hooded sweat shirt, and gloves (the "Suspect"). Shortly thereafter, the Officer observed the Suspect exit the Unity Bank branch while walking quickly. The Suspect got into the rear of a Ford Taurus, which was being driven by a female, bearing New Jersey license plate number X91BVR (the "Ford"). After entering the rear of the Ford, the Suspect crouched down so that he would not be visible to observers.

x. The Officer then followed the Ford, which, after a period of time, attempted to elude the Officer. After the unsuccessful attempt to elude the Officer, the Ford stopped, the Suspect exited the rear of the car, and he pointed his gun at the Officer. At that point, the Officer left the scene.

xi. Thereafter, law enforcement determined that the Ford was registered to an individual named [REDACTED]

[REDACTED]

xii. Real-time location information (including all cell site location and registration information but not including GPS, E-911, or other precise location information) is necessary to locate the user of the Target Facility, which will assist in identifying both Williams's location and the location of the Ford.

xiii. On July 12, 2012, the Honorable Mark Falk, United States Magistrate Judge, issued an Order, attached hereto as Exhibit A, authorizing the FBI to obtain, among other things, real-time location and registration information concerning the Target Facility (including all cell site location information but not including GPS, E-911, or other precise location information).

3. I have been informed that this investigation may require the use of mobile pen register and trap and trace equipment ("the Mobile Equipment") capable of receiving, sending, and capturing the dialing, routing, addressing and signaling information that cellular telephones such as the Target Facility use to establish connections with Sprint's network, and of determining the general direction from which those signals are being broadcast. Generally, the Mobile Equipment may operate by mimicking one of Sprint's cell towers to get the Target Facility to connect to it, or it may simply screen signaling information going to or from Sprint's cell phone towers in the Mobile Equipment's immediate vicinity for dialing, routing, or addressing information emanating from or destined to the Target Facility. Once the Mobile Equipment detects the Target Facility's dialing, routing, addressing or signaling information (by virtue of the Target Facility's unique identifiers described above), the Mobile Equipment may display one or more of the paths from which the Target Facility's signals are received and the strength of those signals. Because radio signals are emitted in all directions and can bounce off, among other

things, structures, the Mobile Equipment cannot definitively identify the direction from which the Target Facility is emitting its dialing, routing, addressing or signaling information. The Mobile Equipment can only identify the path (or paths) from which the Target Facility's signals are being received. The operator of the Mobile Equipment, in turn, may determine the location from which the Target Facility is most likely emitting signals. Because the dialing, routing, addressing, and signaling information contains no content, that information can be obtained using a pen register and trap and trace device.

4. In this instance, the information likely to be obtained from the Mobile Equipment is relevant to the aforementioned investigation because it will enable investigators to attempt to determine the general location of the Target Facility and of the individual or individuals using the Target Facility. 18 U.S.C. § 3122(b)(2).

5. Agents of the Federal Bureau of Investigation have advised that they will deploy and use the Mobile Equipment only from locations where they are lawfully present. They further advise that they will, absent additional lawful authority (such as a search warrant issued pursuant to Fed. R. Crim. P. 41), stop using the Mobile Equipment when it leads them to believe that they have identified a single residence or private space within which the Target Facility may be located. The present application therefore requests authorization for agents of the Federal Bureau of Investigation to deploy mobile pen register and trap and trace equipment to attempt to determine the general location of the Target Facility for a period of 14 consecutive days beginning no later than 10 days from the Court's execution of the proposed Order filed herewith, but not, absent other authority, when they believe they have identified a single residence or private space in which the Target Facility may be located.

6. Because of the way the Mobile Equipment sometimes operates, its use has the potential to intermittently disrupt cellular service to a small fraction of Sprint's wireless customers within its immediate vicinity. Any potential service disruption will be brief and minimized by reasonably limiting the scope and duration of the use of the Mobile Equipment.

7. In order to achieve the investigative objective (i.e., determining the general location of the Target Facility) in a manner that is the least intrusive, data incidentally acquired from phones other than the Target Facility shall not be recorded and/or retained beyond its use to identify or locate the Target Facility.

8. In accordance with Title 18, United States Code, Section 3121(c), the Federal Bureau of Investigation will use the technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to dialing, routing, addressing, and signaling information utilized in the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communication.

9. Because this covert investigation is continuing, premature disclosure of its existence could jeopardize its effectiveness. The Federal Bureau of Investigation considers the Mobile Equipment and its configuration to be Law Enforcement Sensitive. See In re the City of New York, 607 F.3d 923, 942 (2d Cir. 2010); Commonwealth of Puerto Rico v. United States, 490 F.3d 50, 62-64 (1st Cir. 2007); United States v. Van Horn, 789 F.2d 1492, 1508 (11th Cir. 1986).

10. Accordingly, the United States requests that this Court grant an order:

a. authorizing the installation and use of pen register and trap and trace devices without knowledge of, or notification to, the subscriber, to record and decode dialing,

routing, addressing, and signaling information transmitted from the Target Facility, including telephone numbers dialed and pulsed, the date and time of dialings and pulsings, and the length of time the telephone receiver in question is off the hook; and to capture the incoming electronic and other impulses that identify the originating number and other dialing, routing, addressing, and signaling information reasonably likely to identify the source of wire communications to the Target Facility, including caller identification, whenever such electronic and other impulses are sent from or to any location within the jurisdiction of the United States, for the telephones and telephone numbers from which calls are placed to the Target Facility, the date and time of dialings and pulsings, and the length of time the telephone receiver in question is off the hook, for incoming and outgoing calls for a period of 60 days;

b. directing Sprint, a provider of electronic communication service, to furnish agents of the Federal Bureau of Investigation with all information, facilities, and technical assistance necessary to accomplish the installation and use of the pen register and trap and trace device unobtrusively and with minimum interference to the service currently accorded persons whose dialings or pulsings are the subject of the pen register and trap and trace device, including the make and model of the equipment that is associated with or assigned to the Target Facility;

c. directing AT&T, T-Mobile U.S.A., Inc., Verizon Wireless, Metro PCS, Sprint-Nextel and any and all other providers of electronic communication service (hereinafter the "Service Providers") to furnish expeditiously real-time location information concerning the Target Facility (including all cell site location information but not including GPS, E-911, or other precise location information) and, not later than five business days after receipt of a request from

the Federal Bureau of Investigation, all information about subscriber identity, including the name, address, local and long distance telephone connection records, length of service (including start date) and types of service utilized, telephone or instrument number or other subscriber number or identity, and means and source of payment for such service (including any credit card or bank account number), for all subscribers to all telephone numbers, published and non-published, derived from the pen register and trap and trace device during the 60-day period in which the court order is in effect;

d. authorizing agents of the Federal Bureau of Investigation to deploy the Mobile Equipment to monitor the dialing, routing, addressing, and signaling information of the Target Facility in order to determine its general location for a period of 14 consecutive days beginning no later than 10 days from the Court's execution of the proposed Order filed with this Application;

e. directing the Service Providers and their agents, employees, and representatives not to disclose to any person the existence of this application, the court's order, the pen register and trap and trace device, the disclosure of records, or this investigation unless otherwise ordered by the Court; and

f. sealing this application, the court's order, and all papers related to this application unless otherwise ordered by this Court, with the exception of copies of the order necessary for its implementation.

I hereby certify under penalty of perjury that the foregoing is true and correct.

Executed on July 13, 2012.



Osmar J. Benvenuto
Assistant United States Attorney