UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

UNITED STATES OF AMERICA, Plaintiff, -v- ROBERT HARRISON, Defendant.	CRIMINAL NO. 1:14-CR-00170-CCB

AMICI CURIAE MEMORANDUM OF ACLU AND ACLU OF MARYLAND IN SUPPORT OF DEFENDANT ROBERT HARRISON'S MOTIONS TO COMPEL DISCLOSURE OF AND TO SUPPRESS EVIDENCE RELATED TO THE GOVERNMENT'S USE OF A CELL SITE SIMULATOR

TABLE OF CONTENTS

INTRODUCTION

This case involves the surreptitious use of a cell site simulator, more commonly known as a "stingray,"[1] which is a cell phone surveillance device frequently used by law enforcement agencies across the country. These privacy-invasive devices are being employed with little to no oversight from legislative bodies or the courts due to law enforcement secrecy surrounding its use of the technology. Stingrays can be carried by hand, installed in vehicles, or mounted on aircraft.[2] The devices masquerade as the cellular phone towers used by wireless companies such as AT&T and T-Mobile, and in doing so, force *all* mobile phones within the range of the device to emit identifying signals, which can be used to locate not only a particular suspect, but any and all bystanders as well.

In Mr. Harrison's case, Baltimore Police emitted signals into Mr. Harrison's home to force a mobile phone in his possession to transmit its identification and location information. Mot. to Compel 2, ECF No. 28. The government contends that this search was constitutional because it obtained an order from the state court judge, Hon. Barry G. Williams, under the Maryland pen register/trap and trace statute, Md. Code Ann., Cts. & Jud. Proc. § 10-4B-01. Gov't Resp. at 2-3, ECF No. 32. The government further argues that pursuant to the "law enforcement privilege," it is under no obligation to disclose

[1] "StingRay" is the name for a line of cell site simulator technology sold by the Harris Corporation. Other Harris cell site simulator models include the "TriggerFish," "KingFish," and "Hailstorm." Ryan Gallagher, *Meet the Machines That Steal Your Phone's Data*, Ars Technica, Sept. 23, 2013, http://arstechnica.com/tech-policy/2013/09/meet-the-machines-that-steal-your-phones-data. Stingrays, 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 and 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*, Harv. J.L. & Tech. (May 15, 2014), http://ssrn.com/abstract=2437678. Although "StingRay" refers to a specific line of products, *amici* use the term "stingray" in this brief generically to refer to cell site simulators.

[2] Gallagher, *Meet the Machines*, *supra* note 1; *see also* Devlin Barrett, *Americans' Cellphones Targeted in Secret U.S. Spy Program,* Wall St. J. (Nov. 13, 2014), http://online.wsj.com/articles/americans-cellphones-targeted-in-secret-u-s-spy-program-1415917533.

specific information about the stingray device it used to track Mr. Harrison. *Id.* at 6–7. *Amici* explain why these arguments are wrong as a matter of law and corrosive to the judiciary's role in our constitutional system, and therefore must be rejected. *Amici* include publicly available facts about the stingray's capabilities in order to inform the Court of Fourth Amendment concerns unique to this technology, as well as to refute improper claims that the materials Mr. Harrison seeks are privileged.

ARGUMENT

I. USE OF THE STINGRAY VIOLATED THE FOURTH AMENDMENT.

A. Stingray 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 and other wireless devices to the regular telephone network. A stingray masquerades as a wireless carrier's base station, prompting all wireless devices within range to communicate with it. Depending on the particular features of the device and how the operator configures them, stingrays can be used to identify nearby phones,[3] to locate them with extraordinary precision,[4] and can even block service, either to all devices in the area or to particular devices.[5] Stingrays are commonly

[3] A number of companies in addition to the Harris Corporation produce and sell cell site simulator equipment. *See*, *e.g.*, CellXion Ltd., *UGX Series 330: Transportable Dual GSM / Triple UMTS Firewall and Analysis Tool*, http://s3.documentcloud.org/documents/810703/202-cellxion-product-list-ugx-optima-platform.pdf (last visited Oct. 24, 2014) (including as features, "[c]omprehensive identification of IMSI, IMEI and TMSI information"and "[s]imultaneous high speed acquisition of handsets (up to 1500 per minute), across up to five networks").

[4] *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://files.cloudprivacy.net/anchorage-pd-harris-memo.pdf ("[The] system allows law enforcement agencies . . . the ability to . . . [i]dentify location of an active cellular device to within 25 feet of actual location anywhere in the United States.").

[5] *See*, *e.g.*, *UGX Series 330: Transportable Dual GSM / Triple UMTS Firewall and Analysis Tool*, CellXion Ltd., *available at* http://s3.documentcloud.org/documents/810703/202-cellxion-product-list-ugx-optima-platform.pdf (last visited Oct. 24, 2014) (including as features, "[c]omprehensive identification of IMSI, IMEI and TMSI information"and "[s]imultaneous high speed acquisition of handsets (up to 1500 per minute), across up to five networks") (describing device's ability to

used by law enforcement agencies in two ways: to collect the unique international mobile subscriber identity numbers associated with all phones in a given location, or to ascertain the location of a particular phone "when the officers know the numbers associated with it but don't know precisely where it is."[6]

Use of a stingray constitutes a search within the meaning of the Fourth Amendment. Assuming such searches are ever permissible, *see infra* Part I.B, at a minimum they require a warrant based on probable cause. This is so for several reasons.

First, the devices broadcast invisible 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. Stingrays 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, stingrays invade reasonable expectations of privacy. *See Kyllo v. United States*, 533 U.S. 27, 34 (2001) (thermal imaging to detect heat from home constituted search); *United States v. Karo*, 468 U.S. 705, 715 (1984) (monitoring of beeper placed into can of ether that was taken into residence constituted search).[7]

"[d]isable all handsets except operationally friendly"); Miko Mem., *supra* note 4 ("[The] system allows law enforcement agencies . . . the ability to . . . [i]nterrupt service to active cellular connection [and] [p]revent connection to identified cellular device.").

[6] Jennifer Valentino-DeVries, *How 'Stingray' Devices Work*, Wall St. J. (Sept. 21, 2011), http://blogs.wsj.com/digits/2011/09/21/how-stingray-devices-work/.

[7] By way of additional illustration, take the Supreme Court's recent observation that "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 [stingray] 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 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 (quoting *Payton v. New York*, 445 U.S. 573, 590 (1980)).

In addition, stingrays effectively trespass into protected spaces, as they send electronic signals that penetrate the walls of homes and offices in the vicinity in order to seek information about devices in interior spaces. *See Silverman v. United States*, 365 U.S. 505, 509 (1961) (use of "spike mike," a microphone attached to spike inserted into walls of house, constituted "unauthorized physical penetration into the premises" giving rise to a search); *United States v. Jones*, 132 S. Ct. 945, 949 (2012) (installation and monitoring of GPS on suspect's vehicle constituted search because of "physical intrusion" "for the purpose of obtaining information"). No search warrant, let alone a pen register order, would permit the police to search the homes of every house in a neighborhood. Yet, with the stingray, the police can do just that, searching every home, vehicle, purse, and pocket in a given area without anyone ever learning that their devices were searched by the police.

Second, the devices can pinpoint an individual with extraordinary precision, in some cases "with an accuracy of 2 m[eters]."[8] *United States v. Rigmaiden,* a criminal case from the District of Arizona, is one of the few cases in which the government's use of stingrays has been litigated. In it, the government conceded that agents used the device while wandering around an apartment complex on foot, and that the stingray ultimately located the suspect while he was inside his unit. *See United States v. Rigmaiden*, No. CR 08-814-PHX-DGC, 2013 WL 1932800, at *15 (D. Ariz. May 8, 2013). In another case in Florida, *State v. Thomas*, a Tallahassee Police officer testified about how, using a handheld cell site simulator, he "quite literally stood in front of every door and window" in a large apartment complex "evaluating all the handsets in the area" until he narrowed down the specific apartment in which the

[8] *See, e.g.*, PKI Electronic Intelligence GmbH, *GSM Cellular Monitoring Systems*, 12, http://www.pki-electronic.com/2012/wp-content/uploads/2012/08/PKI_Cellular_Monitoring_2010.pdf (device produced by a competitor to the Harris Corporation can "locat[e] ... a target mobile phone within an accuracy of 2 m[eters]").

target phone was located.[9] In Baltimore itself, two people have recently alleged that the government used a stingray device to track their precise locations.[10] In one of the cases, police reportedly used a stingray to track a person within a single city block, and were able to determine that the person carrying the phone was in fact riding on a bus.[11] Accurate electronic location tracking of this type requires a warrant because it intrudes on reasonable expectations of privacy. *Jones*, 132 S. Ct. at 964 (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 v. State*, No. SC11-2254, 2014 WL 5285929, at *19 (Fla. Oct. 16, 2014) ("[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 the Fourth Amendment for which probable cause was required.").

Further, to the extent the government uses stingray devices without a warrant while walking on foot immediately outside people's homes to ascertain information about interior spaces, it impermissibly intrudes on constitutionally protected areas. *See Florida v. Jardines*, 133 S. Ct. 1409 (2013) (government's entry into curtilage with trained dogs to sniff for drug odors emanating from interior of home constitutes search).

Third, stingrays 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* Stip. at 2, ECF No. 32-1. As the Supreme Court explained in no

[9] Transcript of Suppression Hr'g 14, 17, *State v. Thomas*, No. 2008-CF-3350A (Fla. 2d Cir. Ct. Aug. 23, 2010) [hereinafter "*Thomas* Transcript"], *available at* https://www.aclu.org/files/assets/100823_transcription_of_suppression_hearing_complete_0.pdf .

[10] Justin Fenton, *Judge Threatens Detective with Contempt for Declining to Reveal Cellphone Tracking Methods*, Balt. Sun, Nov. 17, 2014, http://www.baltimoresun.com/news/maryland/baltimore-city/bs-md-ci-stingray-officer-contempt-20141117-story.html.

[11] *Id.*

uncertain terms this year, searching the contents of a cell phone requires a warrant. *Riley v. California*, 134 S. Ct. 2473 (2014).

Fourth, Stingrays 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.[12] The government in *Rigmaiden* and *Thomas* conceded as much. *See Rigmaiden*, 2013 WL 1932800, at *20; *Thomas* transcript at 14. This is so even when the government is using a stingray with 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 stingray technology. Thus, when using a stingray the police infringe on the reasonable expectations of privacy of dozens or hundreds 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.[13] *Cf. Berger v. New York*, 388 U.S. 41, 57–59 (1967).

Finally, stingrays can, as a side-effect of their normal use, disrupt the ability of phones in the area to make calls. Harris Corporation, the company that manufactures the StingRay, and at least one of its competitors have apparently taken steps to ensure that 911 emergency calls are not

[12] *See, e.g.*, Hannes Federrath, Multilateral Security in Communications, *Protection in Mobile Communications*, 5 (1999), http://epub.uni-regensburg.de/7382/1/Fede3_99Buch3Mobil.pdf ("possible to determine the IMSIs of all users of a radio cell"); Daehyun Strobel, Seminararbeit, Ruhr-Universität, *IMSI Catcher* (July 13, 2007), http://www.emsec.rub.de/media/crypto/attachments/files/2011/04/imsi_catcher.pdf. ("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.").

[13] *See* Adam Lynn, *Tacoma Police Change How They Seek Permission to Use Cellphone Tracker*, News Tribune, Nov. 15, 2014, http://www.thenewstribune.com/2014/11/15/3488642_tacoma-police-change-how-they.html?sp=/99/289/&rh=1 (explaining that upon learning that police had been using cell site simulators without informing courts of such, judges in Tacoma, Washington, began requiring law enforcement agencies that want to use the devices to swear in affidavits that they will not store data collected from third parties who are not targets of the investigation).

disrupted.[14] However, emergency calls to doctors, psychologists, and family members may be blocked while the stingray is in use nearby. This is invasive in general, raises possible conflicts with federal law, *see* 47 U.S.C. § 333, 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 stingrays must be strictly constrained.

In light of these factors, use of a stingray 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'" (quoting *Katz v. United States*, 389 U.S. 347, 357 (1967)). The government did not obtain a warrant to use a stingray device in this case. In fact, it did not request authorization to use a stingray 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.A. The underlying Order was made pursuant to Maryland's Pen Registers and Trap and Traces Devices Statute, which authorizes installation of such a device "if the court finds that the information likely to be obtained by the installation and use is *relevant to an ongoing criminal investigation*." Md. Code Ann., Cts. & Jud. Proc. § 10-4B-04 (emphasis added). The government's invocation of probable cause in its pen register application[15] and the court's reference to probable cause in the order[16] do not transform a pen register/trap and trace order into a warrant. Warrants require not just a probable cause showing, but also must "describe with particularity the items to be seized [in order to ensure] that a citizen is not subjected

[14] Barrett, *supra* note 2.
[15] Appl. at 2, *In Re Appl. of Md. For an Order Authorizing the Installation & Use of a Device Known as a Pen Register/Trap & Trace Over 443-803-6749,* No. 1:14-cr-00170-CCB (Circ. Ct. Md. Feb. 5, 2014) (Defendant filed this document as ECF No. 29-1)
[16] Order at 1, *In Re Appl. of Md. For an Order Authorizing the Installation & Use of a Device Known as a Pen Register/Trap & Trace Over 443-803-6749,* No. 1:14-cr-00170-CCB (Circ. Ct. Md. Feb. 5, 2014) (Defendant filed this document as ECF No. 29-1)

to 'a general, exploratory rummaging in [his personal] belongings.'" *United States v. Hurwitz*, 459 F.3d 463, 470 (4th Cir. 2006) (quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971)); *see also* Fed. R. Crim. P. 41 (setting out requirements for issuance of a warrant in federal courts); Md. Code Ann., Crim. Proc. § 1-203 (same, for state courts). Warrants also involve a strict requirement of notice to the target of the search, a default requirement that the warrant be executed in the daytime hours, a time limit on execution of the warrant, and other protections. Fed. R. Crim. P. 41 (e)(2)(C)(ii), (f)(2); Md. Code Ann., Crim. Proc. § 1-203 (a)(5)-(6). Moreover, warrants must be accompanied by a sworn affidavit based on personal knowledge of an investigating officer and setting forth the basis for probable cause. Md. Code Ann., Crim. Proc. § 1-203(a)(2)(i)(3); Fed. R. Crim. P. 41(d). The pen register application at issue here was merely signed by a police detective and the facts therein were not sworn to under oath. Because use of a stingray constitutes a search, the government must, at the very least, secure a warrant before employing such a device. The government's insertion of information in support of a finding of probable cause in its Application suggests that it understood these concerns; as such, the government should have applied for a proper search warrant.

B. Even if Baltimore Police had obtained a warrant to use a stingray, which it failed to do, use of the stingray would still raise serious Fourth Amendment concerns.

Even in instances where the government obtains a warrant, stingray 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, stingrays collect identifying and location information about dozens or hundreds of innocent bystanders' phones, send electronic signals through the walls of nearby homes and offices, learn otherwise private information about the locations of phones inside those spaces, and interfere with bystanders' 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). Stingrays, 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."); *Doe v. Broderick*, 225 F.3d 440, 453 (4th Cir. 2000) ("The expectation that one generally remains free from warrantless searches in the privacy of the home is at the heart of the Fourth Amendment, but the Supreme Court has long recognized that searches of office buildings and commercial premises in the absence of a search warrant grounded upon probable cause are unreasonable as well.") (internal citations omitted). Furthermore, interrupting and preventing dozens or hundreds of people's cell phone calls, including urgent and important calls, in the course of tracking a single suspect raises serious questions about the reasonableness of the search. *See United States v. Ramirez*, 523 U.S. 65, 71 (1998).

II. THE GOVERNMENT'S APPLICATION CONTAINED MATERIAL MISREPRESENTATIONS INVALIDATING ANY PURPORTED JUDICIAL AUTHORIZATION TO USE A STINGRAY.

A. The Order authorizing use of the stingray was based on a misleading Application for a pen register/trap and trace device that breached the government's duty of candor to the issuing judge.

The government's stingray search did not fall within the scope of its Application. First, the government misled the court in requesting what appeared to be a run-of-the-mill pen register/trap and

trace order. Second, its Application contained no mention of a stingray device, much less any explanation of how such a device operates, the immense privacy implications for innocent third parties, or the fact that regular use of the stingray can disrupt phone calls nearby.

Courts recognize a pen register as a device that records the numbers dialed by a particular telephone and a trap and trace device as recording the incoming numbers to a telephone. *See Smith v. Maryland*, 442 U.S. 735, 736 & n.1 (1979); *see also* Md. Code Ann., Cts. & Jud. Proc. § 10-4B-01 (c)(1)-(d)(1). The government sought a pen register order to authorize use of a "cellular tracking device," but Maryland's pen register statute makes no provision for, or even mention of, a "cellular tracking device."[17] *See generally,* Appl., *Appl. for Pen Register*, No. 1:14-cr-00170-CCB; Md. Code Ann., Cts. & Jud. Proc. § 10-4B-01. Without a description from the government as to 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 stingray. Even more unlikely would have been the court's independent understanding that unlike a pen register/trap and trace device, a stingray broadcasts signals that penetrate the walls of every private home in its vicinity, and is incapable of targeting only one phone or person, but instead searches every mobile phone in range.

The portion of the government's Application that purportedly sought authorization to use a stingray is vague, brief, and buried in a single paragraph:

[17] Under federal law, pen register orders may not be used to obtain location information. *See* 47 U.S.C. § 1002(a)(2) ("[W]ith regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices . . . , such call identifying information shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number)."). Although the Maryland pen register statute does not include this limiting language, use of information collected under the state statute in a federal prosecution that would not be obtainable using the analogous federal statute raises concerns. Moreover, as of October 1, 2014, law enforcement in Maryland must obtain a 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 Maryland legislature has now clearly forbidden use of a pen register order to obtain real-time location information.

> "...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…"

Appl. at 6-8, *Appl. for Pen Register*, No. 1:14-cr-00170-CCB. There is no explanation of what these "tools" are, how they operate, or how they will be used. In addition, there is absolutely no indication in the Application or the Order that the authorization will subject potentially unlimited numbers of innocent third parties to dragnet surveillance, none of whom will ever receive notice that their phones were tracked, and that the search will intrude into constitutionally protected spaces. The government's lack of specificity fails its duty of candor to the courts. *See United States v. Comprehensive Drug Testing, Inc.* (*CDT*) 621 F.3d 1162, 1176 (9th Cir. 2010) (en banc) (Kozinski, J. concurring) ("A lack of candor in this or any other aspect of the warrant application must bear heavily against the government in the calculus of any subsequent motion to return or suppress the seized data."). By neglecting to apprise the court that it intended to use a stingray, 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 and that all aspects of the search are supported by probable cause, described with particularity, and conducted pursuant to a warrant.

The role of the court in enforcing the requirements of the Fourth Amendment is key. When judges have learned that police departments are seeking to use stingray devices and understood the capabilities of those devices, they have limited the scope of orders and demanded that the government be more candid in its requests.[18] In a recent federal investigation in New Jersey, for example, the government submitted an application for a pen register order to use a stingray that included

[18] Or, they have thrown out evidence altogether. *See supra* note 11.

significantly more detail than was provided in this case, even stating that: the device will "mimic[] one of Sprint's cell towers to get the Target [phone] to connect to it;" "[b]ecause 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;" and "data [will be] incidentally acquired from phones other than the Target." Appl. at 6-8, *Appl. for Pen Register*, No. 1:14-cr-00170-CCB; Order, *Order for Pen Register*, No. 1:14-cr-00170-CCB; *United States v. Williams,* No. 13-00548 (KM) (D.N.J. 2014). Based on this description of the intrusive nature of the technology, and recognizing that a pen register order cannot authorize such an intrusion, the federal magistrate judge reviewing the application modified the government's proposed order by hand to prohibit the government from using the stingray "in any private place or where [FBI agents] have reason to believe the Target [phone] is in a private place." Order at 5, Order for Pen Register, No. 1:14-cr-00170-CCB.

More recently, a local newspaper investigation in Tacoma, Washington, revealed that police had used a stingray more than 170 times over five years but had concealed their intent to do so from judges when seeking court orders.[19] Once local judges learned from a reporter that they had been unwittingly authorizing stingray use, they collectively imposed a requirement that the government spell out whether it is seeking to use a stingray device in future pen register applications.[20] Law enforcement agencies that want to use the device must now swear in affidavits that they will not store data collected from third parties who are not targets of the investigation.[21] Similarly, after the local newspaper in Charlotte, North Carolina, revealed that police had been using stingrays for eight years

[19] Lynn, *Tacoma Police Change How They Seek Permission to Use Cellphone Tracker*, *supra* note 14.
[20] *Id.*
[21] *Id.*

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.[22]

Here, had the government candidly told Judge Williams that it intended to use a stingray, he could have denied the application without prejudice to a subsequent application providing further details about the technology, imposed limits on use of the device, or denied the application and invited the government to apply for a search warrant instead. A federal magistrate judge recently denied a pen register application to use a stingray on these grounds. *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. June 2, 2012). As the same magistrate judge explained in denying a statutory application for cell site records of *all* subscribers from several cell towers, an understanding of "the technology involved" is necessary to "appreciate the constitutional implications of" the government's application, particularly where, as here, the technology entails "a very broad and invasive search affecting likely hundreds of individuals in violation of the Fourth Amendment." *In re Application for an Order Pursuant to 18 U.S.C. § 2703(D)*, 930 F. Supp. 2d 698 (S.D. Tex. 2012).

In another case, a federal magistrate judge denied a pen register application on the ground that use of a stingray is too intrusive because of the impact on third parties. *See In re Application for an Order Authorizing Use of a Cellular Telephone Digital Analyzer*, 885 F.Supp. 197, 201 (C.D. Cal. 1995) (denying statutory application to use stingray because, *inter alia,* "depending upon the effective range of the digital analyzer, telephone numbers and calls made by others than the subjects of the investigation could be inadvertently intercepted"). That stingrays obtain information about third parties

[22] Fred Clasen-Kelly, *CMPD's Cellphone Tracking Cracked High-Profile Cases*, Charlotte Observer, Nov. 22, 2014, www.charlotteobserver.com/2014/11/22/5334827/cmpds-cellphone-tracking-cracked.html.

"creates a serious risk that every warrant for [a stingray] will become, in effect, a general warrant," to search persons as to whom there is no probable cause. *See CDT*, 621 F.3d at 1176.

The government here failed to provide Judge Williams with essential information about the nature and scope of the search it sought to conduct. Indeed, the lack of government candor to the courts and Judge Williams' actual response once apprised of the government's activities is highlighted by two ongoing prosecutions in state court. At a November 17 suppression hearing, Judge Williams threatened to hold a Baltimore Police detective in contempt of court if he did not explain how the city tracked a phone to locate the defendant in that case.[23] The detective refused to respond to the defense attorney's questions about the stingray device used, citing a "nondisclosure agreement" with the FBI.[24] Judge Williams responded that the detective "[does not] have a nondisclosure agreement with the court."[25] After the heated exchange, the prosecution decided to withdraw the phone evidence rather than answer the judge's questions.[26] Likewise, in a September hearing in a different case, Judge Williams pressed a Baltimore police officer to answer the defense's questions about how he tracked a phone to the defendant. *See* Transcript of Suppression Hearing at 29-30, *State of Maryland v. Batty*, Case No. 113078021 (Circ. Ct. Md., Balt. Cnty., Sept. 16, 2014), 29–30. When the officer explained only that "[t]his kind of goes to Homeland Security issues," the judge ordered the tracking evidence excluded, explaining: "I mean, this is simple. You can't just stop someone and not give me a reason, State, and you know that." *Id.* In light of Judge Williams's reaction to government concealment in those cases, it is not unreasonable to believe that had the government given some indication of how it

[23] *See* Fenton, *Judge Threatens Detective With Contempt*, *supra* note 11.
[24] *Id.*
[25] *Id.*
[26] *Id.*

intended to use the pen register order, he would have demanded further information before issuing the order, and may well have denied the application altogether.

The police's tracking of Mr. Harrison's person was invalid due to a misleading application. The government's "lack of candor," was highly consequential to Mr. Harrison's case, and he has a right to corroborate his claims with evidentiary information from the government. *CDT,* 621 F.3d at 1170 (Kozinski, C.J., concurring).

B. The lack of candor in the government's Application requires the court to hold a *Franks* hearing to examine the validity of the court order.

The government's omission of information about the stingray from its Application prevented the court from exercising its constitutional oversight function and renders the Order invalid. At a minimum, Mr. Harrison is entitled to an evidentiary hearing on whether the omission of information about the cell site simulator was intentional and material. *See Franks v. Delaware,* 438 U.S. 154 (1978). A defendant seeking a *Franks* hearing based on omission of information must make a showing that "omissions were '*designed to mislead,* or . . . made in *reckless disregard of whether they would mislead*' and that the omissions were material." *United States v. Clenney*, 631 F.3d 658, 664 (4th Cir. 2011) (alteration and emphasis in original) (quoting *United States v. Colkley*, 899 F.2d 297, 301 (4th Cir.1990)). If the court finds that "'inclusion [of the omitted material] in the affidavit would defeat probable cause,'" *id.*, "the search warrant must be voided and the fruits of the search excluded." *Franks*, 438 U.S. at 155.[27] Although the government obtained and relied on a pen register order, not a warrant, in this case, there is no reason why the *Franks* rule should not apply. A material omission or misrepresentation to the issuing judge should void the order and result in exclusion of evidence gathered pursuant to it.

[27] Courts have consistently held that "[s]uppression remains an appropriate remedy if the magistrate or judge in issuing a warrant was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth." *Leon*, 468 U.S. at 897–98.

The government made serious omissions and misrepresentations with respect to its intended use of a stingray demonstrating a reckless disregard for the truth. It completely left out any description of the type of equipment it was seeking to use; in fact, its Application makes absolutely no mention of a "stingray," "cell site simulator" or "IMSI catcher." Instead, on its face, the government's Application appears to be a routine request for a pen register, which is a completely different surveillance technology with significantly lesser surveillance capabilities than a cell site simulator with none of the side effects inflicted upon innocent third parties.

The misrepresentation in this case is not an isolated incident; law enforcement and prosecutors across the country have systematically concealed information about stingrays from courts. For example, documents obtained from the FBI show that it has a longstanding policy of concealing information about stingrays.[28] An email produced in discovery in *Rigmaiden* stated that the investigative team "need[ed] to develop independent probable cause of the search warrant … FBI does not want to disclose the [redacted] (understandably so)."[29] In the same case, prosecutors conceded that the government had not made a "full disclosure to the magistrate judge [who issued the original order authorizing the surveillance] with respect to the nature and operation of the [StingRay] device [used to locate Rigmaiden]."[30] The reason for that lack of candor, the DOJ later told the court, was "because of the

[28] *See* City's Verified Answer, Affidavit of Bradley S. Morrison at 2, *Hodai v. City of Tucson*, No. C20141225 (Ariz. Super. Ct. Mar. 4, 2014). ("[T]he FBI has, as a matter of policy, for over 10 years, protected this specific electronic surveillance equipment and techniques from disclosure, directing its agents that while the product of the identification or location operation can be disclosed, neither details on the equipment's operation nor the tradecraft involved in use of the equipment may be disclosed.").

[29] Exhibit 34 to Discovery & Suppression Issues at 51, *United States v. Rigmaiden*, 844 F. Supp. 24 982 (D. Ariz. July 27, 2011) (No. 08-cr-00814-DGC) (emphasis added) (Email from Denise L Medrano, Special Agent, Phoenix Field Office, to Albert A. Childress (July 17, 2008 6:01 AM)), https://www.aclunc.org/sites/default/files/Rigmaiden_ECF_No.587-2_Exhibits_34.pdf.

[30] Transcript of Motion to Suppress at 81, *United States v. Rigmaiden*, 844 F. Supp. 2d 982 (D. Ariz. 2012) (No. CR 08-814-PHX-DGC).

sensitive nature of the device in terms of concerns out of the disclosure to third parties."[31] An email released by the U.S. Attorney's Office for the Northern District of California via a Freedom of Information Act request explains that "many" law enforcement agents in that district were using stingrays under the auspices of pen register orders, but without "mak[ing] that explicit" in the application; even worse, this occurred *after* the federal magistrates had expressed "collective concerns" that pen register orders would not suffice to authorize use of the device.[32] As explained above, in Tacoma, Washington, the government obtained more than 170 orders ostensibly justifying stingray use in recent years, but judges did not know that they had been authorizing use of stingrays until informed of such by a local newspaper report.[33] In Florida, police in the Sarasota area released an email showing that, "at the request of U.S. Marshalls [sic]," in warrant affidavits local police officers "simply refer to [information from a cell site simulator] as '. . . information from a confidential source regarding the location of the suspect.' To date this has not been challenged . . . ."[34]

And in Baltimore, police are invoking a secret nondisclosure agreement with the federal government to justify affirmative concealment of information about stingray use from judges and defense counsel.[35]

All of this indicates that the government's omission of information about stingrays—or affirmative misrepresentation that it is instead using a "pen register" device or obtaining information from a "confidential source"—is hardly innocent. It seems clear that misrepresentations and omissions pertaining to the government's use of stingrays are intentional. The issue is not whether the government

[31] *Id.*
[32] Email from Miranda Kane, USACAN, to USACAN-Attorneys-Criminal listserv (May 23, 2011 11:55 AM) https://www.aclu.org/files/assets/doj_emails_on_stingray_requests.pdf.
[33] Lynn, *Tacoma Police Change How They Seek Permission to Use Cellphone Tracker*, *supra* note 14.
[34] Email from Kenneth Castro, Sergeant, Sarasota Police Dep't, to Terry Lewis, (Apr. 15, 2009, 11:25 EST), https://www.aclu.org/sites/default/files/assets/aclu_florida_stingray_police_emails.pdf.
[35] Fenton, *Judge Threatens Detective With Contempt*, *supra* note 11.

should have followed-up on or disclosed facts not of its own making. The government cannot disclaim responsibility for knowing what device it has chosen to use.

Nor can ignorance about the technology excuse any omission. The functioning of the technology has constitutional significance. It is therefore incumbent on the government to understand the technology and disclose it to the courts. *See In re Application for an Order Pursuant to 18 U.S.C. § 2703(D)*, 930 F. Supp. 2d 698 (S.D. Tex. 2012) (rejecting application for so-called "cell tower dump," i.e., all information from specified cell towers: "[I]t is problematic that neither the assistant United States Attorney nor the special agent truly understood the technology involved in the requested applications. Without such an understanding, they cannot appreciate the constitutional implications of their requests. They are essentially asking for a warrant in support of a very broad and invasive search affecting likely hundreds of individuals in violation of the Fourth Amendment.").

Moreover, the government's omissions were material to Judge William's decision to grant the order. *See supra* Part II.A. The government's request seemingly targeted a small group of alleged conspirators, not potentially thousands of innocent parties. Had the government clearly explained that it was not seeking to use a pen register at all, but rather a device that interacts with and searches the phones of many third parties by sending signals through the walls of homes and into private spaces, the court's decision almost certainly would have been affected.

In short, the Application failed to alert the issuing judge that the government intended to use a stingray, misleadingly stated it intended to use a "pen register," and failed to provide basic information about what the technology is and how it works. The omissions were intentional and material. Mr. Harrison is therefore entitled to suppression or a *Franks* hearing, to ensure that the government is not permitted to conduct searches pursuant to an invalid court order.

III. THE LAW ENFORCEMENT PRIVILEGE DOES NOT APPLY IN THIS CASE.

A. The law enforcement privilege is not relevant to the government's use of the stingray.

The government argues that Mr. Harrison's motions to compel disclosure and to suppress evidence should be dismissed on the basis of a "privilege applicable to information about sensitive law-enforcement techniques." Gov't Resp. at 6, ECF No. 32. The government does not, however, support this contention with legal precedent relevant to Mr. Harrison's case, and aside from a single citation to the Supreme Court's decision in *Roviaro v. United States*, 353 U.S. 53 (1957). does not even cite to mandatory case law within this Circuit. In *Roviaro*, the Court recognized a privilege to protect the identity of police informants to secure the important governmental interest in receiving information about criminal events from members of the public. *Id.* at 59. Here, where Mr. Harrison is seeking information about a tool that was used to obtain key evidence in the prosecution's case against him—in violation of the Fourth Amendment—and where information about the device and technique used to gather that evidence is already publicly available and widely known, there is no analogous public interest. Any claims from the government that other investigations will be hampered by disclosure are conclusory, especially in light of public information already available. *See infra* Part III.B.

Other cases cited by the government are likewise unavailing. In *United States v. Harley*, 682 F.2d 1018, 1020 (D.C. Cir. 1982), the D.C. Circuit allowed the government to withhold "the location of a police surveillance post" in order to protect "the safety of the cooperating apartment owner or tenant." The basis for that holding is indistinguishable from the rule set forth in *Rovario*, and no analogous concern applies here. Likewise, in *United States v. Van Horn*, 789 F.2d 1492, 1508 (11th Cir. 1987), the Eleventh Circuit held that the government could withhold the "precise locations where [surveillance cameras] are hidden or their precise specifications." Here, Mr. Harrison does not seek a precise

description of the path police followed while operating the stingray or technical documents detailing its "precise specifications." Rather, he seeks investigative reports, identities of operating officers, and similar records that bear on the nature and scope of the Fourth Amendment violation. And to the extent Mr. Harrison did seek specifications of the stingray device used to locate him, that information is already public and therefore application of the privilege is waived. *Infra* Part III.B.

While the facts of *Roviaro*, involving withholding the identity of a human informant, do not compare with the facts at hand, the Supreme Court did articulate limiting guidance that is instructive here:

> The scope of the privilege is limited by its underlying purpose. Thus, where the disclosure of the contents of a communication will not tend to reveal the identity of an informer, the contents are not privileged. Likewise, *once the identity of the informer has been disclosed* to those who would have cause to resent the communication, *the privilege is no longer applicable*.

Roviaro, 353 U.S. at 60-61 (emphasis added). This Court has likewise recognized a limited privilege, stating, "[t]he purpose behind the privilege is to prevent interference with an on-going investigation," as opposed to an investigation that has been closed. *United States v. Lang*, 766 F. Supp. 389, 404 (D. Md. 1991). To invoke the privilege, police must first "make a substantial threshold showing that there are specific harms likely to accrue from disclosure of specific materials." *Bellamy-Bey v. Baltimore Police Dep't*, 237 F.R.D. 391, 393 (D. Md. 2006). The court then employs a balancing test to weigh "whether 'disclosure of specific information would result in specific harm to identified important interests' against the relevance of the documents to the plaintiff's case and the injury to the public and plaintiff of non-disclosure." *Id.* (citing *King v. Conde*, 121 F.R.D. 180, 190, 198 (E.D.N.Y. 1988)). "The test dictates that '[b]lanket and generalized assertion of privilege is not sufficient to overcome the presumption of discoverability.'" *Martin v. Conner*, 287 F.R.D. 348, 351 (D. Md. 2012) (internal citation omitted).

Here, the government has not made a substantial threshold showing that specific harms will accrue from the disclosure; even had it done so, it has still not shown that those harms would outweigh the potential injury to Mr. Harrison's case.

B. There is an abundance of public information on stingrays such that the technology is no longer secret.

Regardless of whether the government could otherwise meet its burden to invoke the privilege, the abundance of public information on stingrays renders the issue moot. In fact, stingrays have been the subject of front page stories in leading newspapers,[36] featured in Hollywood movies[37] and television dramas,[38] and are even available for sale over the Internet from one of many non-U.S. based surveillance technology vendors.[39] Legal scholars have published lengthy academic articles describing the history of the technology, its use by the government, and its capabilities.[40] Computer science graduate students have even published detailed theses and research papers about the surveillance methods used by the stingray.[41] As much as the Baltimore police and federal agencies would like this technology to be a secret, the reality is that the secret was out a long time ago.

---

[36] *See* Ellen Nakashima, *Little-Known Surveillance Tool Raises Concerns by Judges, Privacy Activists*, Wash. Post (Mar. 27, 2013), http://www.washingtonpost.com/world/national-security/little-known-surveillance-tool-raises-concerns-by-judges-privacy-activists/2013/03/27/8b60e906-9712-11e2-97cd-3d8c1afe4f0f_story.html; Jennifer Valentino-DeVries, *'Stingray' Phone Tracker Fuels Constitutional Clash*, Wall St. J. (Sept. 22, 2011), http://online.wsj.com/article/SB10001424053111904194604576583112723197574.html.

[37] *See* Zero Dark Thirty at 00:80:38 (Sony Pictures 2012).

[38] *See The Wire: Middle Ground* at 00:12:57 (HBO television broadcast Dec. 12, 2004) (dialogue between two characters) ("Remember those analog units we used to use to pull cell numbers out of the air? . . . We used to have to follow the guy around, stay close while he used the phone." "New digitals . . . bing, we just pull the number right off the cell towers.").

[39] *See* Letter from Rep. Alan M. Grayson to Tom Wheeler, Chairman, Fed. Commc'ns Comm'n (July 2, 2014), http://grayson.house.gov/images/pdf/rep_grayson_letter_to_federal_communications_commission_chairman.pdf (making reference to a Chinese online merchant and stating that "IMSI catchers can apparently 'be bought openly' from online retailers for as little as $1800".).

[40] *See* Pell and Soghoian, *Your Secret Stingray's No Secret Anymore*, *supra* note 1; *See also* Heath Hardman, *The Brave New World of Cell-Site Simulators*, Alb. L. Rev. (May 22, 2014), http://dx.doi.org/10.2139/ssrn.2440982.

[41] *See* Dennis Wehrle, *Open Source IMSI-Catcher* (Oct. 28, 2009) (unpublished Masters thesis, University of Freiburg), https://github.com/tom-mayer/imsi-catcher-detection/blob/master/Papers/Thesis%20KS/Ausarbeitung-Dennis_Wehrle.pdf. *See also* Daehyun Strobel, *IMSI Catcher*, 13 (2007) (seminar paper, Ruhr-Universitat Bochum), http://www.emsec.rub.de/media/crypto/attachments/files/2011/04/imsi_catcher.pdf

1. Publicly Available Information about Baltimore Police Department's Stingray(s)

In addition to the vast amount of public information describing the capabilities of the stingray technology, the City of Baltimore has officially documented the Baltimore Police Department's purchase and use of the technology. According to publicly available minutes of Baltimore Board of Estimates meetings, the City has made at least three purchases of cell site simulators and related equipment from the Harris Corporation:

- At the Board's February 4, 2009 meeting, it awarded $132,800 to Harris Corporation for a "Cell Phone Tracking System" for the police department.[42]
- At the Board's June 9, 2010 meeting, it extended its warranty with Harris Corporation for a "Cell Phone Tracking System" for an additional $30,000.[43]
- At the Board's January 23, 2013 meeting, it agreed to pay Harris Corporation $99,786 for a "Hailstorm Cell Phone Tracker Upgrade" on behalf of the police department.[44]

Together, the city has spent over $250,000 for stingray technology, and has disclosed this fact to the public. This disclosure is now widely known, and has been the subject of articles in the Baltimore media and national news outlets.[45]

---

[42] *Available at* http://comptroller.baltimorecity.gov/minutes/2009-02-04.pdf.
[43] *Available at* http://comptroller.baltimorecity.gov/minutes/1767-1899_2010-06-09.pdf
[44] *Available at* http://comptroller.baltimorecity.gov/minutes/0179-0279_2013-01-23.pdf (The Hailstorm is an upgrade to the stingray that enables law enforcement agencies to track modern smartphones that use "4G" the latest mobile network technology.). *See*, Cyrus Farivar, C*ities Scramble to Upgrade "Stingray" Tracking as End of 2G Network Looms*, Ars Technica (Sept. 1, 2014), http://arstechnica.com/tech-policy/2014/09/cities-scramble-to-upgrade-stingray-tracking-as-end-of-2g-network-looms/
[45] The Baltimore Sun recently explained, for example, that "[r]ecords shows [sic] that the Baltimore Police Department purchased a stingray for $133,000 in 2009." Fenton, *Judge Threatens Detective with Contempt*, *supra* note 11. *See also* Gallagher, *Meet the Machines*, *supra* note 1 (citing Baltimore's purchase of a Hailstorm).

2. Public Information About Harris Corporation's Cell Site Simulator Devices

Detailed information about the technical specifications and capabilities of stingrays are also publicly available from patent applications submitted by the Harris Corporation.[46] Harris has even publicly filed photos of its devices with the U.S. Patent and Trademark Office.[47] Harris Corporation's own publicly available promotional materials describe the capabilities and features of its cell site simulators. *See* Appendix A.[48]

Documents made public by state and local governments as part of their cell site simulator procurement processes reveal similar details. For example, the Anchorage, Alaska, Police Department's purchase request for a "Kingfish" cell site simulator describes many of its capabilities, including the ability to:

- Identify location of an active cellular device to within 25 feet of actual location anywhere in the United States;
- Track the route of any active cellular device and record tracking information for evidentiary purposes;
- Mimic the functional appearance of an active cellular service tower
- Interrupt service to active cellular connection; and

[46] Competitors to the Harris Corporation have also published detailed information on how their stingray devices work. *See, e.g.,* PKI, *GSM Cellular Monitoring Systems*, *supra* note 9. *See also*, United States Patent No. 7,592,956, Rodney Keith McPherson & David James Lanza (Inventors), Harris Corp. (Assignee) (Sept. 22, 2009), *available at* http://patft.uspto.gov/netahtml/PTO/search-bool.html (enter"7,592,956" into search field).

[47] *Available at* http://tsdr.uspto.gov/documentviewer?caseId=sn76303503&docId=SPE20130404144554#docIndex=2&page=1; http://tsdr.uspto.gov/documentviewer?caseId=sn77316689&docId=SPE20140514151847#docIndex=1&page=1; http://tsdr.uspto.gov/documentviewer?caseId=sn76303814&docId=SPE20140213150610#docIndex=2&page=1.

[48] *See* Harris, StingRay and AmberJack Product Descriptions, *available at* http://egov.ci.miami.fl.us/Legistarweb/Attachments/34769.pdf; Harris, KingFish Product Description, http://egov.ci.miami.fl.us/Legistarweb/Attachments/34771.pdf at 2; *see also* Gallagher, *Meet the Machines*, supra note 1 (describing Harris Corporation's line of cell site simulators).

- Prevent connection to identified cellular device ("No Service")[49]

3. Information Released by the Federal Government

The federal government itself has released significant information about its use of cell site simulators. In response to a Freedom of Information Act request from the Electronic Privacy Information Center, the U.S. Department of Justice has released thousands of pages of documents about the use of cell site simulators in criminal investigations.[50] Likewise, the Department of Justice Electronic Surveillance Manual describes the capabilities of cell site simulators:

> Law enforcement possesses electronic devices that allow agents to determine the location of certain cellular phones by the electronic signals that they broadcast. This 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. Working together, these devices allow the agent to identify the direction (on a 360 degree display) and signal strength of a particular cellular phone while the user is making a call. By shifting the location of the device, the operator can determine the phone's location more precisely using triangulation.[51]

The Manual also explains the legal process that federal agents are required to obtain in order to use cell site simulators.[52] In addition, the Federal Communications Commission has released information about regulation of cell site simulators, including letters from local police departments seeking permission to use the devices on the public radio spectrum.[53]

---

[49] Memo. From Stephen W. Miko, Anchorage Police Dep't, to Bart Mauldin, Anchorage Police Dep't (June 24, 2009), available at http://files.cloudprivacy.net/anchorage-pd-harris-memo.pdf.
[50] *See* Electronic Privacy Information Center, *EPIC v. FBI – Stingray/Cell Site Simulator*, https://epic.org/foia/fbi/stingray/ (last visited Nov. 24, 2014).
[51] Dep't of Justice, *Electronic Surveillance Manual*, 44 (June 2005), http://www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf.
[52] *See Electronic Investigative Techniques*, U.S. Atty's Bull., Sept. 1997, 13–14 (discussing use of digital analyzers and cell site simulators), http://www.justice.gov/usao/eousa/foia_reading_room/usab4505.pdf.
[53] Letter from Julius P. Knapp, FCC, to Christopher Soghoian (Feb. 29, 2012), *available at* http://files.cloudprivacy.net/FOIA/FCC/fcc-stingray-reply.pdf

4. Information in Judicial Opinions and Records

Judicial opinions and court documents from around the country reveal ample details about how cell site simulators are used in particular investigations. The U.S. District Court for the District of Utah, for example, detailed testimony by an FBI agent describing, step-by-step, how he used a cell site simulator "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." *United States v. Allums*, No. 2:08–CR–30 TS, 2009 WL 806748, at *1 (D. Utah, Mar. 24, 2009). In a Wisconsin case, police officers testified in a suppression hearing in open court about their use of a cell site simulator to track a cell phone signal to a particular apartment building. Motion Hearing Transcript at 13–16, *State v. Tate*, No. 09CF002842 (Wis. Cir. Ct., Apr. 22, 2011), *appeal pending*, No. 2012AP000336-CR (Wis. Argued Oct. 3, 2013). In a federal case in California, the court docketed a copy of the government's application for an order authorizing use of a cell site simulator, which included a detailed description of how the device would be used:

> A cell site simulator is a mobile device that captures the signaling information—the phone number, serial number, etc.—of cell phones within the vicinity. The cell site simulator mimics a cell site tower in that it reads signaling information broadcast in public by cell phones turned on in the area. After locating [the suspect] through physical surveillance, agents will position the cell site simulator nearby. Any cell phone that [the suspect] possesses (if turned on), as well as other cell phones nearby, will transmit their signaling information to the cell site simulator. Agents will repeat the process multiple times at different locations and times. By identifying the signaling data common to each capture—i.e., the signaling information that comes up each time—agents can determine the signaling information for a phone used by [the suspect].

Motion to Suppress Cell Site & Simulated Cell Site Evidence, Ex. B-1 at 2 n.2, *United States v. Espudo* (No. 12-CR-0236-IEG) 954 F. Supp. 2d 1029 (S.D. Cal. filed Apr. 8, 2013). In *Rigmaiden,* the U.S. District Court for the District of Arizona included a list of factual admissions by the government

concerning its use of a cell site simulator in the case. *Rigmaiden*, 844 F. Supp. at 995. A 2013 indictment filed in the Northern District of Illinois describes use of a cell site simulator (called a "digital analyzer device") to identify a suspect's cell phone number. Complaint, Affidavit of Robert Lukens at 8 n.1, *United States v. Arguijo*, No. 13-CR-0155 (N.D. Ill. Feb. 13, 2013). A 2006 opinion from the Southern District of Indiana describes law enforcement's use of a cell site simulator "to pinpoint the multi-unit residence located at [the building address] as the precise location of a particular cell phone believed to be used by or otherwise connected with [the suspect]." *United States v. Bermudez*, No. IP05-0043-CR05-BF, 2006 WL 3197181, at *1 (S.D. Ind. June 30, 2006), *aff'd sub nom. United States v. Amaral-Estrada*, 509 F.3d 820 (7th Cir. 2007). In the District of New Jersey, a search warrant filed on the public docket by the government granted the FBI authority to use a stingray and described in detail its capabilities. Search Warrant to Obtain Location, Other Data, & Telephone Records for a Cellular Telephone Facility, *In Re Application of the United States for the Authorization to Obtain Location Data Concerning a Cellular Tel. Facility Currently Assigned Telephone Number (908) 448-3855*, Mag. No. 12-3092 (D.N.J. 2012). And in Florida, a police officer explained in court, step by step, how he used a stingray in a particular investigation, the capabilities of the device, and its impact on third parties.[54] These and other descriptions of stingray use in public judicial records belie the government's claim that the information Mr. Harrison seeks is privileged.

* * *

The publicly available information about stingrays, including information about the Baltimore Police Department's use of them, fatally undermines the government's claim that information about the stingray in this case cannot be disclosed. *See, e.g.*, Order Unsealing Suppression Hearing Transcript,

[54] *Thomas* Transcript at 10–23, *supra* note 10.

State v. Thomas, Case No. 37 2008-CF-3350A (Fla. 2d Cir. Ct. June 11, 2014). (rejecting government invocation of the law enforcement privilege and ordering information about stingray use in a criminal investigation to be disclosed). This Court should reject the government's attempt to shield important information about the legality and constitutionality of government conduct from public view.

CONCLUSION

For the foregoing reasons, the government's use of the stingray and collection of cell phone location information about Mr. Harrison pursuant to an invalid court order violated the Fourth Amendment and is not subject to a law enforcement exception. *Amici* respectfully urge the court to grant Mr. Harrison's motions to compel disclosure and suppress evidence.

Respectfully submitted,

/s/ David Rocah

David Rocah (Bar No. 27315)
Counsel of Record for Amici
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF MARYLAND
3600 Clipper Mill Rd., Ste. 350
Baltimore, MD 21211
Phone: (410) 889-8555
Email: rocah@aclu-md.org

Nathan Freed Wessler[55]
Of counsel
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad St., 18th Floor
New York, NY 10004
Phone: (212) 549-2500
Email: nwessler@aclu.org

Dated: November 25, 2014

[55] Drafting assistance provided by Samia Hossain, Brennan Fellow, American Civil Liberties Union Foundation, New York, NY (recent law graduate; application for admission to New York State bar to be filed).