NO. 15-CF-322

IN THE DISTRICT OF COLUMBIA COURT OF APPEALS

PRINCE JONES,
Defendant-Appellant,

v.

UNITED STATES OF AMERICA,
***Plaintiff-Appellee*.**

On Appeal from the Superior Court of the District of Columbia Criminal Division, No. 2013-CF1-18140

BRIEF OF THE AMERICAN CIVIL LIBERTIES UNION, AMERICAN CIVIL LIBERTIES UNION OF THE NATION'S CAPITAL, AND ELECTRONIC FRONTIER FOUNDATION AS AMICI CURIAE SUPPORTING THE APPELLANT AND REVERSAL

ARTHUR B. SPITZER
AMERICAN CIVIL LIBERTIES UNION
OF THE NATION'S CAPITAL
4301 Connecticut Avenue, N.W., Suite 434
Washington, D.C. 20008
T: (202) 457-0800
F: (202) 457-0805
artspitzer@aclu-nca.org

JENNIFER LYNCH
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
T: (415) 436-9333
jlynch@eff.org

NATHAN FREED WESSLER
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
T: (212) 549-2500
F: (212) 549-2654
nwessler@aclu.org

Certificate Required by Rule 28(a)(2)

I hereby certify as follows:

Amici American Civil Liberties Union, American Civil Liberties Union of the Nation's Capital, and Electronic Frontier Foundation are non-profit membership corporations. No publicly held corporation owns any of their stock, as they have issued no stock. None of *amici* have parent or subsidiary corporations.

Arthur B. Spitzer
American Civil Liberties Union
of the Nation's Capital
4301 Connecticut Avenue, N.W., Suite 434
Washington, D.C. 20008
T: (202) 457-0800
F: (202) 457-0805
artspitzer@aclu-nca.org

Attorney for Amici Curiae

February 22, 2016

Table of Contents

Interests of Amici viii

Summary of Argument 1

Argument 2

I. Use of the Cell Site Simulator Violated the Fourth Amendment. 2

A. Cell site simulator 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 the MPD had obtained a warrant to use the cell site simulator, use of the device would still raise serious Fourth Amendment concerns. 10

II. In Light of the Government's Excessive Secrecy, This Court Should Hold That, at a Minimum, Cell Site Simulator Use Requires a Warrant; Further, Any Such Warrant Should Include Minimization Rules. 11

A. MPD's Acquisition of Cell Site Simulators. 12

B. Secrecy Surrounding Cell Site Simulator Use Frustrates Judicial Oversight. 14

C. This Court should hold that cell site simulator use requires a warrant that includes protections for bystanders' privacy. 21

Conclusion 25

Appendix 27

Table of Authorities

Cases

Arizona v. Gant, 556 U.S. 332 (2009) 10

**Berger v. New York*, 388 U.S. 41 (1967) 8, 23

California v. Acevedo, 500 U.S. 565 (1991) 9

Commonwealth v. Augustine, 4 N.E.3d 846 (Mass. 2014) 4

Illinois v. Gates, 462 U.S. 213 (1983) 21

**In re Appeal of Application for Search Warrant*, 71 A.3d 1158 (Vt. 2012) 23

In re Application for an Order Authorizing Disclosure of Location Information for a Specified Wireless Telephone, 849 F. Supp. 2d 526 (D. Md. 2011) 4

In re Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device, 890 F. Supp. 2d 747 (S.D. Tex. 2012) 22

In re Application of the U.S. for an Order Authorizing the Monitoring of Geolocation and Cell Site Data for a Sprint Spectrum Cell Phone, Misc. No. 06-0186, 2006 WL 6217584 (D.D.C. Aug. 25, 2006) 4, 22

In re Application of the U.S. for an Order Pursuant to 18 U.S.C. §§ 2703(C) and 2703(D) Directing AT&T, Sprint/Nextel, T-Mobile, MetroPCS and Verizon Wireless to Disclose Cell Tower Log Information, 42 F. Supp. 3d 511 (S.D.N.Y. 2014) 23

**In re Application of the U.S. for an Order Relating to Telephones Used by Suppressed*, No. 15 M 0021, 2015 WL 6871289 (N.D. Ill. Nov. 9, 2015) 3, 8, 23, 24

**Kyllo v. United States*, 533 U.S. 27 (2001) 4, 9, 25

Maryland v. Garrison, 480 U.S. 79 (1987) 11

O'Connor v. Donaldson, 422 U.S. 563 (1975) 21

Payton v. New York, 445 U.S. 573 (1980) 9

Redmond v. State, 213 Md. App. 163 (Md. Ct. Spec. App. 2013) 21

Ricks v. State, 537 A.2d 612 (Md. 1988) 23

**Riley v. California*, 134 S. Ct. 2473 (2014) 5, 6, 9

Smith v. Maryland, 442 U.S. 735 (1979) 4

Stanford v. Texas, 379 U.S. 476 (1965) 11

State v. Earls, 70 A.3d 630 (N.J. 2013) 4, 6

State v. Tate, 849 N.W.2d 798 (Wis. 2014) 5

Thomas v. United States, 914 A.2d 1 (D.C. 2006) 21

**Tracey v. State*, 152 So.3d 504 (Fla. 2014) 3, 6, 9

**United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162 (9th Cir. 2010) 23, 24, 25

United States v. Espudo, 954 F. Supp. 2d 1029 (S.D. Cal. 2013) 22

**United States v. Jones*, 132 S. Ct. 945 (2012) 4, 6, 9

**United States v. Karo*, 468 U.S. 705 (1984) 9

United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010) 9

United States v. Ramirez, 523 U.S. 65 (1998) 10

United States v. Rigmaiden, No. CR 08-814-PHX-DGC, 2013 WL 1932800 (D. Ariz. May 8, 2013) 5

United States v. Warshak, 631 F.3d 266 (6th Cir. 2010) 25

Statutes

18 U.S.C. § 2518 23

18 U.S.C. § 3122 ..... 17, 21

18 U.S.C. § 3125 22

18 U.S.C. § 3127 22

47 U.S.C. § 333 22

47 U.S.C. § 1002 10

Cal. Gov't Code § 53166 25

D.C. Code § 23-547 23

Wash. Rev. Code § 9.73.260 ..... 17, 25

Other Authorities

2014-15 Equity Report, Friendship PCS-Collegiate Academy 8

Adam Lynn, *Tacoma Police Change How They Seek Permission to Use Cellphone Tracker*, News Tribune, Nov. 15, 2014 ..... 15, 17

Alison Knezevich, *Baltimore Co. Police Used Secretive Phone-Tracking Technology 622 Times*, Baltimore Sun, Apr. 9, 2015 16

Brad Heath, *Police Secretly Track Cellphones to Solve Routine Crimes*, USA Today, Aug. 24, 2015 ..... 1, 19, 21

Brief *Amici Curiae* of Electronic Frontier Foundation, ACLU Foundation, and ACLU of Wisconsin, Inc. in Support of Defendant-Appellant, *United States v. Patrick*, No. 15-2443 (7th Cir. Jan. 22, 2016) 21

Center for Human Rights and Privacy, *Non-Disclosure Agreements Between FBI and Local Law Enforcement for StingRay* 15

Cyrus Farivar, *Cities Scramble to Upgrade "Stingray" Tracking as End of 2G Network Looms*, Ars Technica, Sept. 1, 2014 13

Daehyun Strobel, Seminararbeit, Ruhr-Universität, *IMSI Catcher* (July 13, 2007) 7

Dep't of Justice Policy Guidance: Use of Cell-Site Simulator Technology (Sept. 3, 2015) 3, 5, 7, 10

Department of Employment Services, http://does.dc.gov/ 7

Devlin Barrett, *Americans' Cellphones Targeted in Secret U.S. Spy Program*, Wall St. J., Nov. 13, 2014 ..... 1, 10

District of Columbia Office of Contracting and Procurement, Contract Award Details, Contract No. FA0P3000598 (Mar. 17, 2003) 7, 12

District of Columbia Office of Contracting and Procurement, Contract Award Details, Contract No. FAOP2-812 (May 31, 2002) 12

Ellen Nakashima, *Secrecy Around Police Surveillance Equipment Proves a Case's Undoing*, Wash. Post, Feb. 22, 2015 20

Fred Clasen-Kelly, *CMPD's Cellphone Tracking Cracked High-Profile Cases*, Charlotte Observer, Nov. 22, 2014 ..... 16, 17

Glenn E. Rice, *Secret Cellphone Tracking Device Used by Police Stings Civil Libertarians*, Kan. City Star, Sept. 5, 2015 16

Government Cellphone Surveillance Catalogue, The Intercept (posted Dec. 17, 2015) 7, 12

Hannes Federrath, Multilateral Security in Communications, *Protection in Mobile Communications* (1999) 7

Jack Gillum & Eileen Sullivan, *US Pushing Local Cops to Stay Mum on Surveillance*, Associated Press, June 12, 2014 1

Jason Leopold, *DC Police, the FBI, and Their Secret Agreement to Hide Cell Phone Spying*, Vice News, Sept. 30, 2015 14

Jason Leopold, *Police in Washington, DC Are Using the Secretive 'Stingray' Cell Phone Tracking Tool*, Vice News, Oct. 17, 2014 ..... 12, 13

Jennifer Valentino-DeVries, *How 'Stingray' Devices Work*, Wall St. J. (Sept. 21, 2011) 3

Jeremy Scahill & Margot Williams, *Stingrays: A Secret Catalogue of Government Gear for Spying on Your Cellphone*, The Intercept, Dec. 17, 2015 7

Joel Kurth, *Michigan State Police Using Cell Snooping Devices*, Detroit News, Oct. 23, 2015 16

Joseph Goldstein, *New York Police Dept. Has Used Cellphone Tracking Devices Since 2008, Civil Liberties Group Says*, N.Y. Times, Feb. 11, 2016 15

Justin Fenton, *Baltimore Police Used Secret Technology to Track Cellphones in Thousands of Cases*, Baltimore Sun, Apr. 9, 2015 16

Justin Fenton, *Judge Threatens Detective with Contempt for Declining to Reveal Cellphone Tracking Methods*, Balt. Sun, Nov. 17, 2014 ..... 5, 20

Kim Zetter, *Feds Admit Stingrays Can Disrupt Cell Service of Bystanders*, Wired, Mar. 1, 2015 2

Kim Zetter, *Turns Out Police Stingray Spy Tools Can Indeed Record Calls*, Wired, Oct. 28, 2015 3

Linda Lye, *Justice Department Emails Show Feds Were Less Than "Explicit" with Judges on Cell Phone Tracking Tool*, ACLU of Northern California, Mar. 27, 2013 18

Log of Tallahassee Police Department Use of Cell Site Simulators, Released Pursuant to ACLU Public Records Request 15

Maria Kayanan, *Internal Police Emails Show Efforts to Hide Use of Cell Phone Tracking*, Free Future Blog, ACLU, June 19, 2014 20

Matt Richtel, *A Police Gadget Tracks Phones? Shhh! It's Secret*, N.Y. Times, Mar. 15, 2015 1

Mem. from Stephen W. Miko, Resource Manager, Anchorage Police Department, to Bart Mauldin, Purchasing Officer, Anchorage Police Department (June 24, 2009) 2

Nathan Freed Wessler, *ACLU-Obtained Documents Reveal Breadth of Secretive Stingray Use in Florida*, Free Future Blog, ACLU, Feb. 22, 2015 20

Nathan Freed Wessler, *New Evidence Shows Milwaukee Police Hide Stingray Usage From Courts and Defense*, Free Future Blog, ACLU, Jan. 25, 2016 16

New Developments in Sacramento "Stingray" Case, ABC 10, Jan. 8, 2016 ..... 16, 18

Park 7, 4020 Minnesota Ave NE, Washington, DC 20019, Apartments.com 7

PKI Electronic Intelligence GmbH, *GSM Cellular Monitoring Systems* 2, 5

Purchase Orders 2010, PO321482, District of Columbia Open Data Catalogue 13

Purchase Orders 2013, PO458505, District of Columbia Open Data Catalogue 14

Robert Patrick, *Controversial Secret Phone Tracker Figured in Dropped St. Louis Case*, St. Louis Post-Dispatch, Apr. 19, 2015 20

Ryan Gallagher, *Meet the Machines That Steal Your Phone's Data*, Ars Technica, Sept. 25, 2013 ..... 1, 12

Staff of Permanent Subcomm. on Investigations, S. Comm. on Homeland Security & Governmental Affairs, 112th Cong., Federal Support for and Involvement in State and Local Fusion Centers (Comm. Print 2012) 13

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 (2014) 1

Stipulation, *United States v. Harrison*, No. 14 Cr. 170 (D. Md. Nov. 7, 2014) 6, 27

Tr. of Official Proceedings, *State v. Andrews*, Nos. 114149007–009 (Balt. City Cir. Ct., Md., June 4, 2015) 5, 8

Tr. of Suppression Hr'g, *State v. Thomas*, No. 2008-CF-3350A (Fla. 2d Cir. Ct. Aug. 23, 2010) 5

U.S. Dep't of Homeland Sec., Policy Directive 047-02 (Oct. 19, 2015) 25

Interests of Amici[1]

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 American Civil Liberties Union of the Nation's Capital ("ACLU-NCA") is the Washington, D.C., affiliate of the ACLU. The protection of privacy as guaranteed by the Fourth Amendment is of special concern to both organizations. The ACLU and ACLU-NCA have been at the forefront of numerous cases addressing the right of privacy, and have filed briefs as direct counsel and *amicus curiae* in cases involving GPS and 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. 1958 (2013); *United States v. Jones*, 132 S. Ct. 945 (2012; *City of Ontario v. Quon*, 560 U.S. 746 (2010).

[1] In accordance with Rule 29(a), all parties have consented to the filing of this brief. No party or counsel for a party authored this brief in whole or in part, and no person or entity other than the *amici* made any monetary contribution intended to fund the preparation or submission of this brief.

Summary of Argument

This case involves the surreptitious use of a cell site simulator, a cell phone surveillance device commonly known as a "Stingray."[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 a deliberate policy of secrecy.[3] Cell site simulators can be installed in vehicles, mounted on aircraft, or even carried by hand.[4] They masquerade as the cellular tower antennas of 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, Metropolitan Police Department ("MPD") officers transmitted signals through the walls of homes and vehicles in a Washington, D.C., neighborhood to force Defendant's mobile phone to transmit its unique serial number and, as a result, reveal its location. In the process, MPD also collected data about an unknown number of bystanders'

---

[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, bit.ly/1mkumNf. Other companies selling cell site simulators to domestic law enforcement agencies include Boeing subsidiary Digital Receiver Technology (DRT). *See* Devlin Barrett, *Americans' Cellphones Targeted in Secret U.S. Spy Program,* Wall St. J., Nov. 13, 2014, on.wsj.com/1EHIEez. 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).

[3] *See* Brad Heath, *Police Secretly Track Cellphones to Solve Routine Crimes*, USA Today, Aug. 24, 2015, usat.ly/1LtSLdI; Matt Richtel, *A Police Gadget Tracks Phones? Shhh! It's Secret*, N.Y. Times, Mar. 15, 2015, nyti.ms/1BLgbVA; Jack Gillum & Eileen Sullivan, *US Pushing Local Cops to Stay Mum on Surveillance*, Associated Press, June 12, 2014, yhoo.it/1KfUXWw.

[4] Gallagher, *supra* note 2; *see also* Barrett, *supra* note 2.

phones. *Amici* submit this brief to provide publicly available facts about cell site simulators' capabilities to inform the Court of Fourth Amendment concerns unique to this technology. *Amici* also explain why, in light of the extreme secrecy surrounding law enforcement use of cell site simulators in the District, it is crucial that the Court provide guidance to police, prosecutors, and the public about the Fourth Amendment's application to cell site simulator surveillance, even if the Court could resolve the case without reaching the merits of this issue.

Argument

I. Use of the Cell Site Simulator Violated the Fourth Amendment.

A. Cell site simulator 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 towers or "cell sites," that connect cell phones to the telephone network. Cell site simulators masquerade as a wireless carrier's base station, prompting all wireless devices within range that use the impersonated wireless carrier to communicate with it.[5] 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,[6] and even to block service to devices in the area.[7] Cell site simulators are commonly used by law enforcement agencies in two ways: to collect the unique electronic serial numbers associated with all phones in a given area, or, as in

[5] Cell site simulators available to law enforcement can be configured to track a phone on any of the carrier networks.

[6] *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).

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

this case, to locate a particular phone "when the officers know the numbers associated with it but don't know precisely where it is."[8] Some versions of the technology can also obtain metadata about a suspect's calls and text messages or even the contents of those communications,[9] although *amici* do not know whether the MPD has employed such capabilities.

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. As explained by the U.S. Department of Justice, "[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* (N.D. Ill. Opinion), No. 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."). In other words, the cell site simulator used in this case did not passively intercept the signals transmitted between Defendant's phone and AT&T'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]

---

[8] Jennifer Valentino-DeVries, *How 'Stingray' Devices Work*, Wall St. J. (Sept. 21, 2011), http://on.wsj.com/1D2IWcw.

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

[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*

This dynamic is essential to understanding the Fourth Amendment status of cell site simulator technology. It means that the "third-party doctrine," as set out in *Smith v. Maryland*, 442 U.S. 735 (1979), is wholly inapposite. That case involved law enforcement's obtaining from the phone company information about the phone numbers a suspect was dialing—information that was already in the company's possession. Unlike dialed phone numbers transiting the phone company's network, the location information in this case was obtained by an MPD 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 cell site simulator to solicit and receive data from a cell phone. Both involve direct collection of information by police, not requests for data already held by a third party.[11]

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

---

Order Authorizing Disclosure of Location Information for a Specified Wireless Telephone, 849 F. Supp. 2d 526, 539–43 (D. Md. 2011) (same); *see also, e.g.*, *In re Application of the U.S. for an Order Authorizing the Monitoring of Geolocation and Cell Site Data for a Sprint Spectrum Cell Phone*, Misc. No. 06-0186, 2006 WL 6217584, at *4 (D.D.C. Aug. 25, 2006) (as a matter of statutory interpretation, real-time cell phone location tracking requires warrant).

[11] Moreover, courts have rejected application of the third-party doctrine to other methods of location tracking. *See, e.g.*, *Commonwealth v. Augustine*, 4 N.E.3d 846, 862–63 (Mass. 2014) (historical cell site location information); *State v. Earls*, 70 A.3d 630, 641–42 (N.J. 2013) (real-time cell phone location tracking via phone company); *see also United States v. Jones*, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) ("[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.").

recently expressed that, absent exigent or exceptional circumstances, a warrant is required. DOJ Guidance at 3.

First, the devices can pinpoint an individual with extraordinary precision, in some cases "with an accuracy of 2 m[eters]."[12] As Sergeant Perkins testified, the cell site simulator model used by MPD in this case displayed the direction and distance of the target phone, allowing police to locate the defendant in a parked car in a busy neighborhood. (Tr. 10/17/14 at 45–46, 49, 98–99). In cases across the country, law enforcement agents have used cell site simulators to precisely pinpoint suspects' locations, including in specific apartments or areas within large apartment complexes. *See, e.g.*, *State v. Tate*, 849 N.W.2d 798, 804 (Wis. 2014) (tracked phone to southeast corner of apartment building); *United States v. Rigmaiden*, No. CR 08-814-PHX-DGC, 2013 WL 1932800, at *15 (D. Ariz. May 8, 2013) (located cellular aircard "precisely within Defendant's apartment"); Tr. of Official Proceedings at 56–58, *State v. Andrews*, Nos. 114149007–009 (Balt. City Cir. Ct., Md., June 4, 2015), *available at* bit.ly/1S125bI (located phone in single apartment in 30–35-unit apartment building); Tr. of Suppression Hr'g at 15–18, *State v. Thomas*, No. 2008-CF-3350A (Fla. 2d Cir. Ct. Aug. 23, 2010), *available at* bit.ly/1jYUgUT (identified "the particular area of the apartment that the handset [signal] was emanating from"). In one Baltimore case, police reportedly used a cell site simulator to determine 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

[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, bsun.md/1uE8k7v.

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 the Fourth Amendment for which probable cause was required."); *Earls*, 70 A.3d at 642 (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.").

Second, 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* (Tr. 10/17/14 at 97–98 (discussing collection of electronic serial numbers)); Stipulation, *United States v. Harrison*, No. 14 Cr. 170 (D. Md. Nov. 7, 2014), ECF No. 32-1 (attached as Appendix 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.

Third, cell site simulators impact third parties on a significant scale. In particular, as defense expert Ben Levitan testified below, (Tr. 10/29/14 at 284–85), 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. *See also* DOJ Guidance at 5.[14] This is so even when the government is using a cell site simulator with the intent to locate or track a particular suspect; collection of innocent bystanders' phone-identifying data and location information is an inherent feature of current cell site simulator technology.

The StingRay, one of the Harris Corporation's cell site simulator models purchased by MPD,[15] has an advertised range of 200 meters.[16] Police operated the cell site simulator in this case for 30–45 minutes while they drove around Northeast D.C., ending at the 4000 block of Minnesota Avenue NE. (Tr. 10/17/14 at 48, 95). Any functioning cell phone on the impersonated network within range of the device as it roamed the streets would have been forced to broadcast identifying data to the MPD. This would include many of the customers and employees of the strip mall, convenience stores, Auto Zone, and other businesses on the 4000 block of Minnesota Ave. (*Id.* at 94). It would have included residents of the 376-unit apartment building at 4020 Minnesota Ave NE and other nearby residences,[17] city employees and District-resident jobseekers at the Department of Employment Services office at 4058 Minnesota Ave,[18] students

[14] *See also, e.g.*, Hannes Federrath, Multilateral Security in Communications, *Protection in Mobile Communications*, 5 (1999), 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), 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.").

[15] *See* District of Columbia Office of Contracting and Procurement, Contract Award Details, Contract No. FA0P3000598 (Mar. 17, 2003), http://app.ocp.dc.gov/RUI/information/award/award_detail.asp?award_id=1331 (detailing purchase of Stingray from Harris Corporation).

[16] *Government Cellphone Surveillance Catalogue*, The Intercept (posted Dec. 17, 2015), bit.ly/1SgIDs6. Other cell site simulator models have larger ranges, sometimes reaching for miles. *Id.*; *see also* Jeremy Scahill & Margot Williams, *Stingrays: A Secret Catalogue of Government Gear for Spying on Your Cellphone*, The Intercept, Dec. 17, 2015, bit.ly/1O9s5dK.

[17] *See* Park 7, 4020 Minnesota Ave NE, Washington, DC 20019, Apartments.com, bit.ly/23yyryA.

[18] *See* Department of Employment Services, http://does.dc.gov/.

and staff of the nearly 900-student Friendship Collegiate Academy at 4095 Minnesota Ave,[19] and rail and bus riders transiting through the Minnesota Avenue Metro Station. As Sgt. Perkins agreed, "this is a place where there are a lot of people at." (Tr. 10/17/14 at 95). It is impossible to know how many people were affected as police drove the cell site simulator towards Capitol Heights, then toward Kenilworth Avenue, then along Minnesota Avenue, among other locations. (*Id.* at 95–96).

Thus, when using a cell site simulator the police infringe on the reasonable expectations of privacy of large numbers of 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. *See infra* Part II.C (discussing minimization requirements that should accompany cell site simulator warrants); *see also N.D. Ill. Opinion*, 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).

Fourth, 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. *See, e.g.*, Tr. of Official Proceedings at 49, *State v. Andrews*, Nos. 114149007–009 (Balt. City Cir. Ct., Md., June 4, 2015) ("Q And it sends an electronic transmission through the wall of that house, correct? A Yes."). 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

[19] *See* 2014-15 Equity Report, Friendship PCS-Collegiate Academy, 1.usa.gov/1TscxbO.

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).[20] Even in a case like this one, where the suspect was tracked to his car rather than his home, the Fourth Amendment privacy interests are significant.[21] Because "no police officer would be able to know *in advance* whether" the device will invade the privacy of a home, the search "is presumptively unreasonable without a warrant." *Kyllo*, 533 U.S. at 39–40. No search warrant would permit the police to search the interior of every house in a neighborhood. Yet, with the cell site simulator, the police can do just that, searching inside every home, vehicle, purse, and pocket in a given area without anyone ever learning that their privacy was invaded by the police.

Fifth, as a side effect of their normal use, cell site simulators disrupt the ability of cell phones in the area to make and receive calls. (Tr. 10/17/14 at 44 ("Once [the cell site

[20] By way of further illustration, "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*, 134 S. Ct. at 2490. 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 U.S. at 38. To protect such intimate details, "the Fourth Amendment draws 'a firm line at the entrance to the house.'" *Id.* at 40 (quoting *Payton v. New York*, 445 U.S. 573, 590 (1980)).

[21] The automobile exception to the warrant requirement, which allows searches of the contents of vehicles without a warrant, *see California v. Acevedo*, 500 U.S. 565, 579–80 (1991), says nothing about whether a warrant is required to track a person's location to his or her vehicle. *See United States v. Maynard*, 615 F.3d 544, 567 (D.C. Cir. 2010) (rejecting application of automobile exception to warrantless GPS tracking of a vehicle), *aff'd sub nom Jones*, 132 S. Ct. 945; *see also Tracey*, 152 So.3d at 526 (using real-time cell phone location tracking to follow suspect's travels requires a warrant, even if it turns out the suspect is in his car). Moreover, even when a *suspect* is tracked to a location where she has a reduced expectation of privacy, the privacy interests of *bystanders* in their homes and other constitutionally protected spaces are unmitigated.

simulator] grabs [a phone] and holds on to it for a minute, it cannot contact immediately with an actual Sprint tower"); *id.* at 103); DOJ Guidance at 5 ("[T]he target cellular device (*e.g.*, cell phone) and other cellular devices in the area might experience a temporary disruption of service from the service provider."). The Harris Corporation, the company that manufactures the cell site simulators purchased by MPD, has apparently taken steps to ensure that 911 calls are not disrupted. Barrett, *supra* note 2. However, urgent calls to doctors, psychologists, workplaces and family members may be blocked while the cell site simulator is in use nearby. This is true both for the target of the search and for bystanders. Zetter, *supra* note 7. 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 potentially enormous consequences for anyone trying to make an urgent call. 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, taking these effects into account.

In light of these factors, use of a cell site simulator is presumptively unconstitutional unless the government obtains a valid warrant based on probable cause. *See Arizona v. Gant*, 556 U.S. 332, 338 (2009) (explaining that warrantless searches are "*per se* unreasonable"). The government did not obtain a warrant to use a cell site simulator device in this case, and its claim of exigency was correctly rejected by the Superior Court. (Tr. 10/29/14 at 310). This Court should hold that MPD's use of the cell site simulator violated the Fourth Amendment.

B. Even if the MPD had obtained a warrant to use the cell site simulator, 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 dragnet search 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: lack of particularity and overbreadth. *See Maryland v. Garrison*, 480 U.S. 79, 84 (1987) ("By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the [particularity] requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit.").

II. In Light of the Government's Excessive Secrecy, This Court Should Hold That, at a Minimum, Cell Site Simulator Use Requires a Warrant; Further, Any Such Warrant Should Include Minimization Rules.

For years, the Metropolitan Police Department has shrouded its acquisition and use of cell site simulators in extraordinary secrecy, including by entering into an agreement with the Federal Bureau of Investigation to conceal relevant information from judges, defense attorneys, and the public.[22] Although skeletal details about MPD's acquisition of cell site simulators are now known, the Department continues to conceal significant information, which explains the dearth of opportunities for courts in the District to address the issue. Because MPD's policy of

[22] *See infra* note 36 and accompanying text.

concealment has until now prevented judicial consideration of the issues raised in this appeal, and is likely to continue to frustrate review in the future, this Court should rule on the underlying Fourth Amendment issue in this case. It should do so even if the Court ultimately resolves this case as the trial court did, in a manner that does not require ruling on the warrant issue. Without such a ruling, police, prosecutors, Superior Court judges and magistrates, and the public will be without guidance about the Fourth Amendment's limits on an invasive and frequently deployed surreptitious electronic surveillance technique.

A. MPD's Acquisition of Cell Site Simulators.

According to public procurement records, in 2002 and 2003 the District spent more than $200,000 purchasing Triggerfish and Stingray cell site simulators from the Harris Corporation.[23] Both devices mimic cellular tower antennas, allowing police to track, locate, and surveil cell phones.[24] As described in an internal MPD memorandum released under the Freedom of Information Act, although MPD paid for the Stingray using a federal Homeland Security grant, the agency initially lacked funds to train officers in the its operation.[25] As a result, the technology remained "stored in the Electronic Surveillance Unit equipment vault" until a request

[23] *See* District of Columbia Office of Contracting and Procurement, Contract Award Details, Contract No. FAOP2-812 (May 31, 2002), http://app.ocp.dc.gov/RUI/information/award/award_detail.asp?award_id=435 (showing purchase of Triggerfish for $95,300); District of Columbia Office of Contracting and Procurement, Contract Award Details, Contract No. FA0P3000598 (Mar. 17, 2003), app.ocp.dc.gov/RUI/information/award/award_detail.asp?award_id=1331 (showing purchase of Stingray for $110,572).

[24] *See* Gallagher, *supra* note 2 (describing Harris Corporation's cell site simulator models); Government Cellphone Surveillance Catalogue, *supra* note 16 (providing details about Stingray's capabilities and effects).

[25] Jason Leopold, *Police in Washington, DC Are Using the Secretive 'Stingray' Cell Phone Tracking Tool*, Vice News, Oct. 17, 2014, bit.ly/1swyeZS; Memo from Chief of Police, MPD, re: Outside Training Request for Members of the Electronic Surveillance Unit and Members of the Homicide Branch to Attend [redacted] (Dec. 17, 2008) [hereinafter "MPD Memo"], Appendix Ex. B.

to train officers using a federal Department of Justice grant was approved in 2009.[26] MPD also began the "process of upgrading the [device] and procuring additional equipment to allow the system to function completely" at that time.[27] In seeking approval for those purchases, the Department explained the purpose and function of the technology: "to track cellular phones possessed by criminal offenders and/or suspected terrorists by using wireless technology to triangulate the location of the phone. The ability to [redacted] in the possession of criminals will allow MPD to track their exact movements, as well as pinpoint their current locations for rapid apprehension."[28]

In 2010, MPD used a federal Department of Homeland Security grant to purchase $260,935 in cell site simulator equipment and upgrades from the Harris Corporation.[29] Although specific descriptions of the purchased equipment are redacted in publicly available documents,[30] MPD likely upgraded its existing Stingray to a Stingray II or Hailstorm device.[31] (The Hailstorm upgrade allows police to track cell phones operating on the 4G/LTE network).[32] MPD continued

[26] MPD Memo at 1–3.

[27] *Id.* at 2.

[28] *Id.*

[29] Appendix Ex. C (MPD purchase records); Staff of Permanent Subcomm. on Investigations, S. Comm. on Homeland Security & Governmental Affairs, 112th Cong., Federal Support for and Involvement in State and Local Fusion Centers, 81 (Comm. Print 2012), 1.usa.gov/1JMTAP7 ("[MPD] bought . . . the cell phone tracking and surveillance system for $260,935.").

[30] *See generally* Leopold, *Police in Washington, DC*, *supra* note 25; *see also, e.g.*, Appendix Ex. C.

[31] MPD misleadingly described the 2010 purchase as "COMPUTER SOFTWARE FOR MICROCOMPUTERS" in the District's Purchase Order database. *See* Purchase Orders 2010, PO321482, *available at* District of Columbia Open Data Catalogue, http://data.octo.dc.gov. Records released under FOIA and described in a U.S. Senate committee report make clear, however, that the purchase was of cell site simulator equipment. *Supra* note 29.

[32] Cyrus Farivar, *Cities Scramble to Upgrade "Stingray" Tracking as End of 2G Network Looms*, Ars Technica, Sept. 1, 2014, bit.ly/1x6QKwY.

its acquisition of cell site simulator equipment more recently, with a purchase of $148,314 in "SURVEILLANCE AND COUNTER SURVEILLANCE EQUIPMENT AND SUPPLIES" from the Harris Corporation in 2013,[33] and more than $20,000 in cell site simulator training and maintenance packages in 2014.[34] MPD did not announce any of these purchases at the time.

B. Secrecy Surrounding Cell Site Simulator Use Frustrates Judicial Oversight.

The foregoing, plus the record in this case, is the extent of publicly available information about MPD's acquisition and use of cell site simulators. Despite MPD spending hundreds of thousands of dollars on the technology, training at least five officers in its use, *see* Appendix Exs. D–E, and having two cell site simulators in separate trucks on hand for tracking Defendant in this case, (Tr. 10/17/14 at 65–68),[35] *amici* know of no other case in which MPD has disclosed its use of the equipment. If the frequency of use of this technology by other police departments is any indication, this is not the only D.C. case where a cell site simulator was used. *See infra*.

The lack of disclosure, and thus the dearth of previous court challenges, is troublesome, though not surprising. In 2012, MPD entered into an agreement with the FBI to keep its purchases and use of cell site simulators secret.[36] MPD agreed to "not distribute, disseminate, or otherwise disclose any information concerning the wireless collection equipment/technology. . . to the public." NDA at 2. It also agreed to conceal information from courts and defense counsel:

---

[33] Purchase Orders 2013, PO458505, *available at* District of Columbia Open Data Catalogue, http://data.octo.dc.gov/.

[34] Appendix Ex. D (MPD purchase records).

[35] The cell site simulator in one of the police trucks was out of order during the tracking of Defendant. (Tr. 10/17/14 at 66).

[36] Re: Acquisition of Wireless Collection Equipment/Technology and Non-Disclosure Obligations [hereinafter "NDA"] (Aug. 17, 2012), attached as Appendix Ex. F; Jason Leopold, *DC Police, the FBI, and Their Secret Agreement to Hide Cell Phone Spying*, Vice News, Sept. 30, 2015, bit.ly/1FIhwB6.

> The Metro DC Police Department shall not, in any civil or criminal proceeding, use or provide any information concerning the Harris Corporation wireless collection equipment/technology . . . beyond the evidentiary results obtained through the use of the equipment/technology, including, but not limited to, during pre-trial matters, in search warrants and related affidavits, in discovery, in response to court ordered disclosure, in other affidavits, in grand jury hearings, in the State's case-in-chief, rebuttal, or on appeal, or in testimony in any phase of civil or criminal trial, without the prior written approval of the FBI.

Id. at 3. Perhaps most incredibly, MPD agreed that it "will, at the request of the FBI, seek dismissal of the case in lieu of using or providing, or allowing others to use or provide, any information concerning the Harris Corporation wireless collection equipment/technology . . . (beyond the evidentiary results obtained through the use of the equipment/technology)." *Id.*

MPD is by no means the only police department to have entered into such an agreement with the FBI; state and local law enforcement agencies from Boston to San Diego have done the same.[37] The experience of other jurisdictions helps illustrate the effects of this agreement in facilitating concealment of information from courts and defense counsel. In jurisdiction after jurisdiction, law enforcement has been using cell site simulators with regularity, but intentionally sidestepping disclosure obligations and the duty of candor to the courts.

Records from police departments that have disclosed information about their use of cell site simulators show that the equipment is typically used with frequency. In Tallahassee, Florida, for example, the police department used cell site simulators to track 277 phones over a six-and-a-half-year period.[38] In Tacoma, Washington, it was more than 170 times in five years,[39] and in

[37] Center for Human Rights and Privacy, *Non-Disclosure Agreements Between FBI and Local Law Enforcement for StingRay*, bit.ly/1Wb4u21 (non-disclosure agreements from 19 agencies).

[38] Log of Tallahassee Police Department Use of Cell Site Simulators, Released Pursuant to ACLU Public Records Request, bit.ly/1nTR4N3.

[39] Adam Lynn, *Tacoma Police Change How They Seek Permission to Use Cellphone Tracker*, News Tribune, Nov. 15, 2014, bit.ly/1T4FHeA.

New York City more than 1,000 times over seven years.[40] The Michigan State Police used cell site simulators 128 times in a recent one-year period,[41] and in Kansas City, Missouri, police had used them 97 times as of 2015.[42] The Milwaukee Police Department used cell site simulators in 579 investigations over five years,[43] and the Charlotte-Mecklenburg Police Department in North Carolina did so more than 500 times over a similar period.[44] The Sacramento Sheriff's Department initially estimated that it used cell site simulators in about 500 criminal cases, but later said it could be up to 10,000.[45] The Baltimore Police Department has used the devices in approximately 4,300 investigations since 2007,[46] while the Baltimore County Police Department used cell site simulators 622 times over five years.[47]

Police departments consistently hid these frequent deployments from judges and defense counsel, however, meaning that it has been exceedingly rare for courts to have an opportunity to rule on the constitutionality of cell site simulator surveillance. The overwhelming majority of publicly available examples of applications for court orders by state and local authorities fail to

---

[40] Joseph Goldstein, *New York Police Dept. Has Used Cellphone Tracking Devices Since 2008, Civil Liberties Group Says*, N.Y. Times, Feb. 11, 2016, nyti.ms/1Ke5sd1.

[41] Joel Kurth, *Michigan State Police Using Cell Snooping Devices*, Detroit News, Oct. 23, 2015, detne.ws/1Lr9nQD.

[42] Glenn E. Rice, *Secret Cellphone Tracking Device Used by Police Stings Civil Libertarians*, Kan. City Star, Sept. 5, 2015, bit.ly/1N0Fxo3.

[43] Nathan Freed Wessler, *New Evidence Shows Milwaukee Police Hide Stingray Usage From Courts and Defense*, Free Future Blog, ACLU, Jan. 25, 2016, bit.ly/1QzaH8d.

[44] Fred Clasen-Kelly, *CMPD's Cellphone Tracking Cracked High-Profile Cases*, Charlotte Observer, Nov. 22, 2014, bit.ly/20bOkfh.

[45] *New Developments in Sacramento "Stingray" Case*, ABC 10, Jan. 8, 2016, bit.ly/1TscWLq.

[46] Justin Fenton, *Baltimore Police Used Secret Technology to Track Cellphones in Thousands of Cases*, Baltimore Sun, Apr. 9, 2015, bsun.md/1GS5MJO.

[47] Alison Knezevich, *Baltimore Co. Police Used Secretive Phone-Tracking Technology 622 Times*, Baltimore Sun, Apr. 9, 2015, bsun.md/1PnMot0.

explain that police intended to use a cell site simulator, the capabilities of the device, or its effects on bystanders' phones. Law enforcement agents have generally applied for pen register orders rather than warrants,[48] and those pen register applications have appeared on their face to seek authority to obtain information, including cell phone location information, from the suspect's cellular service provider. They have not put judges on notice that police intended to use their own device that bypasses the phone company, queries multiple phones in the area, and pinpoints phones even within constitutionally protected spaces. Thus, for example, in Tacoma, Washington, judges "unwittingly signed more than 170 orders" without knowing "that they'd been authorizing Tacoma police to use a device capable of tracking someone's cellphone" because "police never mentioned they intended to use the device when detectives swore out affidavits seeking so-called 'pen register, trap and trace' orders allowing them to gather information about a suspect's cellphone use and location."[49] After a local newspaper investigation revealed that police had relied on these orders to justify cell site simulator use, 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.[50] Those rules and others were later enshrined in state law. Wash. Rev. Code § 9.73.260.

In Charlotte, "[t]he court orders that authorize the surveillance do not mention StingRays or explain that the device captures cellphone data from both criminal suspects and innocent people."[51] It was only after reading about law enforcement's use of cell site simulators in the

[48] Pen register orders are issued upon a showing "that the information likely to be obtained is relevant to an ongoing criminal investigation," 18 U.S.C. § 3122(b)(2), rather than the probable cause required for a warrant.

[49] Lynn, *Tacoma Police Change*, *supra* note 39.

[50] *Id.*

[51] Clasen-Kelly, *CMPD's Cellphone Tracking*, *supra* note 44.

surveillance. It was a first for police."[52] In Sacramento, law enforcement "never told judges or prosecutors that they were using the so-called 'cell site simulators' - nor did they specifically ask for permission to use one."[53] In the Northern District of California, federal prosecutors acknowledged that they had been submitting pen register applications to federal magistrate judges to justify cell site simulator use, "although the pen register application[s] do[] not make that explicit."[54] The Department of Justice has since recognized that such dissembling is inappropriate, and now requires that "applications for the use of a cell-site simulator [filed by DOJ personnel] must include sufficient information to ensure that the courts are aware that the technology may be used." DOJ Policy at 5.

A Baltimore case now on appeal illustrates the typical lack of government candor. The pen register application submitted by police in the case primarily sought authority to obtain information from a cellular service provider. In a single paragraph, the government additionally sought permission to "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 . . . ."[55] The application contained no explanation of what these "tools" were, how they operated, how they would be used, or that they would intrude into constitutionally protected spaces and impact the privacy of bystanders by forcing their phones to broadcast information. In response to discovery requests,

---

[52] *Id.*

[53] *New Developments in Sacramento "Stingray"Case*, *supra* note 45.

[54] Linda Lye, *Justice Department Emails Show Feds Were Less Than "Explicit" with Judges on Cell Phone Tracking Tool*, ACLU of Northern California, Mar. 27, 2013, bit.ly/1nTRbrZ.

[55] Application, *In re Application of the State of Maryland for an Order Authorizing the Installation and Use of a Device Known as a Pen Register/Trap & Trace Over 443-208-2776*, at 4–5 (Cir. Ct. for Balt. City, Md., May 5, 2014), attached as Appendix Ex. G.

bystanders by forcing their phones to broadcast information. In response to discovery requests, initially "Baltimore's State's Attorney's Office said it had no information about whether a [cell site simulator] phone tracker had been used in the case. . . . In May, prosecutors reversed course and said the police had used one."[56] The trial court granted the resulting suppression motion, holding that the pen register order "d[id] not authorize the use of the Hailstorm [cell site simulator]" because the operation of a cell site simulator "is very different from what the court order[allows], which is that information that the phone is generating on its own be gathered."[57] The court further held that police should have sought a probable cause warrant.[58]

In Baltimore, as elsewhere, the ability of defense counsel to confirm that a cell site simulator had been used and to challenge it before trial was the rare case. At all stages of investigations and court proceedings, from pen register applications and resulting investigative reports, to subsequent arrest warrant affidavits and court hearings, law enforcement has generally hidden its use of cell site simulators. An investigation by USA Today found that across hundreds of cases in Baltimore, police "concealed" their use of cell site simulators "from the suspects, their lawyers and even judges":

> In court records, police routinely described the phone surveillance in vague terms — if they mentioned it at all. In some cases, officers said only that they used "advanced directional finding equipment" or "sophisticated electronic equipment" to find a suspect. In others, the police merely said they had "located" a suspect's phone without describing how, or they suggested they happened to be in the right place at the right time.[59]

---

[56] Heath, *Police Secretly Track Cellphones to Solve Routine Crimes*, *supra* note 3.

[57] Tr. of Official Proceedings at 36, *State v. Andrews*, No. 114149007–09 (Cir. Ct. for Balt. City, Md., Aug. 20, 2015), *available at* bit.ly/1Sci6Mh, *appeal pending*, No. 1496 (Md. Ct. Spec. App.).

[58] *Id.* at 45–46.

[59] Heath, *Police Secretly Track Cellphones to Solve Routine Crimes*, *supra* note 3.

Baltimore police officers have also refused to answer questions under oath in pretrial hearings, citing "Homeland Security issues" and the non-disclosure agreement with the FBI, and prosecutors have withdrawn cell site simulator-derived evidence rather than see judges sanction those refusals to answer with contempt findings or exclusion of evidence.[60]

Similarly, in Sarasota, Florida, internal police emails show that, at the request of the U.S. Marshals Service, local law enforcement omitted mention of cell site simulators from probable cause affidavits, reports, and depositions. Instead, their practice was to say they had "received information from a confidential source regarding the location of the suspect."[61] In a Tallahassee case where cell site simulator use was later revealed, a police officer under deposition would say only that "covert investigative techniques were used to locate the cell phone," and refused to "go into detail" to describe them.[62] Investigative reports from other Tallahassee cases where police used cell site simulators omit mention of the technology, instead alluding only to use of "electronic surveillance measures," "confidential intelligence," or nothing at all.[63]

In apparent deference to the FBI non-disclosure agreement, prosecutors have even dropped charges or offered unexpectedly favorable plea deals to defendants to avoid complying with discovery orders or requests.[64] The government's obfuscation has extended to cases on

---

[60] Fenton, *Judge Threatens Detective with Contempt*, *supra* note 13.

[61] Maria Kayanan, *Internal Police Emails Show Efforts to Hide Use of Cell Phone Tracking*, Free Future Blog, ACLU, June 19, 2014, bit.ly/1SgJau5.

[62] *See* Def.'s Mot. to Compel Disclosure of Evidence, *State v. Thomas*, No. 2008-CF-3350 (Fla. 2d Cir. Ct. Aug. 2, 2010), attached as Appendix Ex. H.

[63] Nathan Freed Wessler, *ACLU-Obtained Documents Reveal Breadth of Secretive Stingray Use in Florida*, Free Future Blog, ACLU, Feb. 22, 2015, bit.ly/1VvZyV7.

[64] Robert Patrick, *Controversial Secret Phone Tracker Figured in Dropped St. Louis Case*, St. Louis Post-Dispatch, Apr. 19, 2015, bit.ly/1nTRhj4; Ellen Nakashima, *Secrecy Around Police Surveillance Equipment Proves a Case's Undoing*, Wash. Post, Feb. 22, 2015, wapo.st/1K7cKfX.

appeal, where appellate courts have been left by the government to believe that phones were located via requests to the service provider instead of with a cell site simulator, and were thereby prevented from addressing the Fourth Amendment questions at stake.[65]

C. This Court should hold that cell site simulator use requires a warrant that includes protections for bystanders' privacy.

The extraordinary efforts of law enforcement agencies to avoid disclosing information about their cell site simulator use to courts and defense counsel helps explain why the issue has not previously been adjudicated in courts in the District. There is no way to know when, if ever, defense counsel will again be able to smoke out MPD's use of a cell site simulator to locate a defendant. The question of how the Fourth Amendment's warrant requirement applies to cell site simulator surveillance is properly presented to the Court in this case, and the Court should take the opportunity to rule on the issue.[66] This case presents a "novel question of law whose resolution is necessary to guide future action by law enforcement officers and magistrates." *Illinois v. Gates*, 462 U.S. 213, 264, 265 n.18 (1983) (White, J., concurring) (citing *O'Connor v. Donaldson*, 422 U.S. 563 (1975)). Without a ruling, the Fourth Amendment rights of District residents will remain vulnerable to violation.

It is not clear what kind of judicial authorization, if any, MPD has been seeking before using its cell site simulators, but the government's statements in this case indicate that it believes a pen register order, which is issued upon a showing of mere relevance, 18 U.S.C. § 3122(b)(2),

---

[65] *See* Brief *Amici Curiae* of Electronic Frontier Foundation, ACLU Foundation, and ACLU of Wisconsin, Inc. in Support of Defendant-Appellant at 18–23, *United States v. Patrick*, No. 15-2443 (7th Cir. Jan. 22, 2016), *available at* bit.ly/1LhJbG4 (identifying likely cell site simulator use in Seventh Circuit case where the government had not disclosed it in its filings or disclosures before the district court); 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)).

[66] *Cf. Thomas v. United States*, 914 A.2d 1, 8 n.7, 20, 23–24 (D.C. 2006) ("address[ing] the constitutional question" first, even when denying relief to defendant on other grounds).

law enforcement cell site simulators are considered pen registers." (Tr. 10/29/2014 at 252; *accord id.* at 253, 288). This is incorrect. A "pen register" may be used to "record[] or decode[] dialing, routing, addressing, or signaling information transmitted by" a phone, 18 U.S.C. § 3127(3), but may not be used to gather "any information that may disclose the physical location of the subscriber," 47 U.S.C. § 1002(a)(2). Therefore, for purely statutory reasons, a pen register order cannot authorize use of a cell site simulator to track and locate a cell phone. Rather, a warrant is required.[67] *See United States v. Espudo*, 954 F. Supp. 2d 1029, 1039 (S.D. Cal. 2013) ("As cell site location data would disclose the physical location of a subscriber, [47 U.S.C. § 1002] clearly prohibits the government from obtaining it solely on the authority of the Pen/Trap statute."); *In re Application of the U.S. for an Order Authorizing the Monitoring of Geolocation and Cell Site Data for a Sprint Spectrum Cell Phone*, Misc. No. 06-0186, 2006 WL 6217584, at *4 (D.D.C. Aug. 25, 2006) (similar); *In re Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device*, 890 F. Supp. 2d 747, 752 (S.D. Tex. 2012) ("Based on the statutory language and the limited case law analyzing this issue, a pen register does not apply to this type of electronic surveillance [using a cell site simulator]."). More importantly, the Fourth Amendment requires a warrant as well. *See supra* Part I. To the extent MPD has been relying on pen register orders to justify cell site simulator use, it has been in violation of both the pen register statute and the Constitution.

[67] Even to the extent the government thought it could operate its cell site simulator under the authority of the pen register statute, the emergency provision of the law requires that police retroactively apply for a court order "within forty-eight hours" of the emergency deployment. 18 U.S.C. § 3125(a). The government failed to do so here, "constitut[ing] a violation of" federal law. *Id.* § 3125(c).

Even putting aside the substantial question of whether cell site simulators can ever be used consistently with the Fourth Amendment, *see supra* Part I.B, simply holding that a warrant is required may not be enough. Although a plain probable cause warrant can help address the Fourth Amendment interests of the government's surveillance target, it will likely not protect the rights of bystanders whose phones are ensnared by the cell site simulator. To this end, at a minimum any cell site simulator warrant must include provisions to minimize collection, retention, and use of bystanders' data. "Warrants for electronic surveillance routinely set out 'minimization' requirements—procedures for how and under what conditions the electronic surveillance may be conducted."[68] *In re Appeal of Application for Search Warrant*, 71 A.3d 1158, 1170 (Vt. 2012). Because electronic surveillance can sweep in huge quantities of data, such limitations can be important "mechanisms for ensuring the particularity of a search." *Id.*

A recent opinion by a federal magistrate judge in the Northern District of Illinois provides guideposts for such protections: "First, law enforcement officers must make reasonable efforts to minimize the capture of signals emitted from cell phones used by people other than the target of the investigation." *N.D. Ill. Opinion*, 2015 WL 6871289, at *3. This could be achieved

[68] The need to include such protections in electronic surveillance orders is well established. *See, e.g.*, *Berger*, 388 U.S. at 59–60 (explaining need for limits on wiretap orders to avoid overbroad collection); *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1176–77 (9th Cir. 2010) (en banc) (per curiam) (discussing importance of limiting instructions in search warrants for electronic data to protect the privacy of third parties whose records are intermingled with the suspects'); *Ricks v. State*, 537 A.2d 612, 621 (Md. 1988) (describing minimization procedures applied to video surveillance, including when, where, and for how long police can operate the camera, in order to protect "communications and activities not otherwise subject to the order"); *In re Application of the U.S. for an Order Pursuant to 18 U.S.C. §§ 2703(C) and 2703(D) Directing AT&T, Sprint/Nextel, T-Mobile, MetroPCS and Verizon Wireless to Disclose Cell Tower Log Information*, 42 F. Supp. 3d 511, 519 (S.D.N.Y. 2014) (conditioning grant of order for cell tower dump records on sufficiency of "protocol to address how the Government will handle the private information of innocent third-parties whose data is retrieved"); 18 U.S.C. § 2518(5) (requiring minimization of collection of non-pertinent conversations through a wiretap); D.C. Code § 23-547(g) (same).

through technical means such as limiting the broadcast strength of a cell site simulator or using a directional antenna instead of an omnidirectional one, if feasible given the capabilities of the device in use and the facts of the investigation. It could also be achieved by identifying the location of the target as precisely as possible before deploying the cell site simulator, including by requesting cell phone location information from the service provider pursuant to a warrant. Second, to the extent possible, the cell site simulator should be configured so that investigatory personnel cannot view or access third-party data. If such information must be viewed for investigative reasons, it should be accessed only by "specialized personnel or an independent third party." *Comprehensive Drug Testing*, 621 F.3d at 1180 (Kozinski, J., concurring); *accord id.* at 1172 (en banc).

Third, unless retention is required to comply with disclosure obligations to a defendant, "law enforcement officers must immediately destroy all data other than the data identifying the cell phone used by the target. . . . Additionally, the destruction must be evidenced by a verification provided to the Court with the return of the warrant." *N.D. Ill. Opinion*, 2015 WL 6871289, at *4. Fourth, in all cases, "law enforcement officers are prohibited from using any data acquired beyond that necessary to determine the cell phone information of the target. A cell-site simulator is simply too powerful of a device to be used and the information captured by it too vast to allow its use without specific authorization from a fully informed court." *Id.* This means that, even with a separate, later-issued warrant, law enforcement cannot access bystander data that was beyond the scope of the original warrant.

These requirements are reasonable and necessary. Indeed, the U.S. Departments of Justice and Homeland Security already require prompt deletion of bystander data collected by a cell site simulator, providing that "[w]hen the equipment is used to locate a known cellular

device, all data must be deleted as soon as that device is located, and no less than once daily." DOJ Guidance at 6; *accord* U.S. Dep't of Homeland Sec., Policy Directive 047-02, at 7 (Oct. 19, 2015), http://1.usa.gov/1mqvY88. A Washington State statute passed unanimously by the legislature last year similarly requires deletion of bystanders' data, as well as "all steps necessary to limit the collection of any information or metadata to the target specified in the applicable court order." Wash. Rev. Code § 9.73.260(6)(c), as amended by 2015 Wash. Legis. Serv. Ch. 222 (West); *see also* Cal. Gov't Code § 53166(b)(2)(F) (requiring adoption of rules governing destruction of data acquired by a cell site simulator). Similar protections have been imposed by courts in the context of other types of invasive electronic searches. *See supra* note 68; *Comprehensive Drug Testing*, 621 F.3d at 1178–80 (Kozinski, C.J., concurring) (for computer searches, "[t]he government's search protocol must be designed to uncover only the information for which it has probable cause," "[t]he government must destroy or . . . return non-responsive data," and "the government [should] waive reliance upon the plain view doctrine" for non-pertinent evidence).

"The Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish." *United States v. Warshak*, 631 F.3d 266, 285 (6th Cir. 2010). This case presents the Court with an opportunity to conform MPD's surreptitious use of an invasive surveillance device to the requirements of the Constitution. The Court should not let this opportunity pass, lest it "permit police technology to erode the privacy guaranteed by the Fourth Amendment." *Kyllo*, 533 U.S. at 34.

Conclusion

For the foregoing reasons, *amici* urge the Court to hold that the government violated the Fourth Amendment by warrantlessly tracking Defendant's cell phone with a cell site simulator.

February 22, 2016

Respectfully submitted,

Arthur B. Spitzer
American Civil Liberties Union
of the Nation's Capital
4301 Connecticut Avenue, N.W., Suite 434
Washington, D.C. 20008
T: (202) 457-0800
F: (202) 457-0805
artspitzer@aclu-nca.org

Nathan Freed Wessler
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
T: (212) 549-2500
F: (212) 549-2654
nwessler@aclu.org

Jennifer Lynch
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
T: (415) 436-9333
jlynch@eff.org

APPENDIX

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

B. Memo from Chief of Police, MPD, re: Outside Training Request for Members of the Electronic Surveillance Unit and Members of the Homicide Branch to Attend [redacted] (Dec. 17, 2008)…….…App. 4

C. District of Columbia Order No: PO321482 -1FASH8 – NSID [redacted] (Jan. 27, 2010)…….App. 8

D. District of Columbia Order No: PO494686-V2 –FY14-FA0[redacted] Training-[redacted] (Apr. 17, 2014); District of Columbia Order No : PO494200 –FY14-FA0-Maintenance for [redacted] (Apr. 2, 2014)…….....App. 12

E. District of Columbia Order No: PO287717 –[redacted] 2009- Grant fundeed [*sic*] (Jan. 29, 2009)……...App. 17

F. Re: Acquisition of Wireless Collection Equipment/Technology and Non-Disclosure Obligations (Aug. 17, 2012)……...App. 20

G. Application, *In re Application of the State of Maryland for an Order Authorizing the Installation and Use of a Device Known as a Pen Register/Trap & Trace Over 443-208 -2776* (Cir. Ct. for Balt. City, Md., May 5, 2014)……..…….....App. 27

H. Def's Mot. to Compel Disclosure of Evidence, *State v. Thomas*, No. 2008-CF-3350 (Fla. 2d Cir. Ct. Aug. 2, 2010)……...…….App. 39

A

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

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

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

****

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.

B

Memo from Chief of Police, MPD, re: Outside Training Request for Members of the Electronic Surveillance Unit and Members of the Homicide Branch to Attend [redacted] (Dec. 17, 2008)

☑ APPROVED

PURPA 368

Metropolitan Police Department
Investigative Services Bureau
Narcotics and Special Investigations Division

OK 1/9/09

December 17, 2008

MEMORANDUM

Approved A/C 1-9-09

TO: Chief of Police
Executive Office of the Chief of Police

THRU: Executive Director
Resource Accountability

THRU: Assistant Chief of Police
Professional Development Bureau

THRU: Director
Metropolitan Police Academy

THRU: Assistant Chief of Police
Investigative Services Bureau 1-7-09

ATTN: Marcella Clark OK - M 1/8/08
Grant Programs Administration TEAM 8F/08

FROM: Commander
Narcotics and Special Investigations Division Inspector 12-17-08

SUBJECT: Outside Training Request for Members of the Electronic Surveillance Unit and Members of the Homicide Branch to Attend [redacted]

METROPOLITAN POLICE DEPT. OFFICE OF THE C.F.O. 2009 JAN 13 PM 1:29

In 2003, the Metropolitan Police Department (MPD) acquired the [redacted] through a Homeland Security grant. At the time that these systems were procured by the department, no funding was available to train members on the use and maintenance of the systems.

For several years, the systems were stored in the Electronic Surveillance Unit equipment vault. Due to the fact that no MPD personnel had been trained on these systems, the equipment has never been utilized.

FA $ 09 B TEA 8F 2711 $ 0402 4020 12,900

AN

The Narcotics and Special Investigations Division is currently in the process of upgrading the [redacted] and procuring additional equipment to allow the system to function completely.

The [redacted] will be used by MPD to track cellular phones possessed by criminal offenders and/ or suspected terrorists by using wireless technology to triangulate the location of the phone. The ability to [redacted] in the possession of criminals will allow MPD to track their exact movements, as well as pinpoint their current locations for rapid apprehension. The procurement of this equipment will increase the number of MPD arrests for fugitives, drug traffickers, and violent offenders (robbery, ADW, Homicide), while reducing the time it takes to locate dangerous offenders that need to be removed from the streets of DC.

The intelligence gathered by this equipment can be readily shared between MPD and our TEAM DC Federal partners (FBI, DEA, ICE, U.S. Marshals Service, United States Attorney's Office), as well as our neighboring state and local law enforcement agencies. Upon request, this equipment can also be used to assist these agencies with the location and apprehension of any of their targeted offenders.

In reference to a proposal to upgrade the [redacted] that is currently owned by the Metropolitan Police Department, this request is being submitted to authorize four (4) members of the Metropolitan Police Department to attend the [redacted] Course that is being offered by Harris Industries [redacted] during the period of February 3, 2009, through February 10, 2009. This training class is a six (6) day course that runs from Tuesday to Friday during the first week of February, and on Monday and Tuesday during the second week of February.

The following MPD personnel have been selected to attend this training:

[redacted]	CID- Homicide Branch
[redacted]	NSID- Electronic Surveillance Unit
[redacted]	CID- Homicide Branch
[redacted]	NSID- Electronic Surveillance Unit

The training course is designed to provide students with an in-depth knowledge of the operation and maintenance of the [redacted]

The training course will be held at the Harris Industries Satellite Office, located in Chantilly, Virginia.

The cost of this training course is [redacted], for a total of [redacted] Due to the fact that the training is being held in the Washington Metropolitan Area, there are no other costs associated with this course.

It is requested that forty-eight (48) hours of Administrative Leave be granted for these members to attend this training course.

The cost of this training course will be funded through the Edward Byrne Violent Crime Targeting Initiative (TEAM DC), which is administered by the Bureau of Justice Assistance. Obligated Service Agreements and a DC Training Form 1 are attached for each member. Thank you for your consideration of this request.

C

District of Columbia Order No : PO321482 -1FASH8 – NSID [redacted]
(Jan. 27, 2010)

[redacted]

Order No : PO321482 -1FASH8 - NSID [redacted]

Issued on Wed, 27 Jan, 2010

Supplier:
HARRIS CORPORATION
1025 W. NASA BLVD.
MELBOURNE, FL 32919
United States
Phone: 1321.727.5391
Fax: 1321.727.5677
Contact: [redacted]

Ship To:
Metropolitan Police Department
2235 Shannon Pl., SE
Washington, DC 20020
United States

Bill To:
State Homeland Security Grant
300 Indiana Ave., NW RM:# 4106
Washington, DC 20001
United States
Phone: 1Main (202)727-5298
Fax: 1Fax (202)727-4845

Deliver To:
Insp. Brian Bray, (202) 698-5505

If used in conjunction with a contract award, purchase order is placed in accordance with all provisions of Contract Number: N/A
Bill To Contact: [redacted]
Requester: [redacted]
Form:
Delivery Date: Thu, 30 Apr, 2009
PR No.: RQ558382

Item	Description	Part Number	Unit	Qty	Need By	Unit Price	Extended Amount
1	[redacted]	[redacted]	each	1	Thu, 30 Apr, 2009	[redacted]SD	[redacted]USD

Item	Description	Part Number	Unit	Qty	Need By	Unit Price	Extended Amount
2	[redacted]	[redacted]	each	1	Thu, 30 Apr, 2009	[redacted]USD	[redacted]SD

Item	Description	Part Number	Unit	Qty	Need	Unit Price	Extended Amount

					By		
3	[redacted]	[redacted]	each	3	Thu, 30 Apr, 2009	[redacted]00USD	[redacted]USD

Item	Description	Part Number	Unit	Qty	Need By	Unit Price	Extended Amount
4	[redacted]	[redacted]	each	1	Thu, 30 Apr, 2009	[redacted]00USD	[redacted]SD

Item	Description	Part Number	Unit	Qty	Need By	Unit Price	Extended Amount
5	[redacted]	[redacted]	[redacted]	1	[redacted] Apr, 2009	[redacted]	

Item	Description	Part Number	Unit	Qty	Need By	Unit Price	Extended Amount
6	[redacted]	[redacted]	each	1	Thu, 30 Apr, 2009	[redacted]USD	[redacted]SD

Item	Description	Part Number	Unit	Qty	Need By	Unit Price	Extended Amount
7	[redacted]	[redacted]	each	1	Thu, 30 Apr, 2009	[redacted]USD	[redacted]

Item	Description	Part Number	Unit	Qty	Need By	Unit Price	Extended Amount
8	[redacted]	[redacted]	each	1	Thu, 30 Apr, 2009	[redacted]USD	[redacted]USD

Item	Description	Part Number	Unit	Qty	Need By	Unit Price	Extended Amount
9	[redacted]	[redacted]	each	1	Thu, 30 Apr, 2009	[redacted]0USD	[redacted]

Item	Description	Part Number	Unit	Qty	Need By	Unit Price	Extended Amount
10	[redacted]	[redacted]	each	3	Thu, 30 Apr, 2009	[redacted] USD	[redacted] USD
					Total		$260,935.00USD

Comments

- APPROVED by [redacted] on *Friday, January 22, 2010 at 11:28 AM* with comment (2 documents attached)
  This requisition has been processed in accordance with applicable laws, regulations and policies/procedures and is ready for approval

  Contractor shall provide [redacted] accordance with the Contractor's attached Quote No. QTE6779-02290, dated January 21, 2010, which is hereby incorporated and made part of the purchase order. This order is subject to the attached Contractor's Terms and Conditions of Sale for Wireless Equipment, Software and Services. Delivery shall be made not later than 120 days after receipt of the purchase order by the Contractor [redacted] Fri, 22 Jan. 2010)
- COMMENT by **Ariba System** on *Wednesday, January 27, 2010 at 11:53 AM*
  FOB is Destination unless specified otherwise (aribasystem, Wed, 27 Jan, 2010)
- COMMENT by **Ariba System** on *Wednesday, January 27, 2010 at 11:53 AM*
  *****GOVERNMENT OF THE DISTRICT OF COLUMBIA STANDARD CONTRACT PROVISIONS FOR USE WITH THE DISTRICT OF COLUMBIA GOVERNMENT SUPPLY AND SERVICES CONTRACTS ARE HEREBY INCORPORATED BY REFERENCE. WWW.OCP.DC.GOV***** (aribasystem, Wed, 27 Jan, 2010)
- COMMENT by **Ariba System** on *Wednesday, January 27, 2010 at 11:53 AM*
  ALL INVOICES SHALL BE SUBMITTED TO THE 'BILL TO' ADDRESS INDICATED ON THIS PURCHASE ORDER. INVOICES SHALL INCLUDE THE PURCHASE ORDER NUMBER, CONTRACT NUMBER (IF APPLICABLE), CONTRACTOR'S NAME AND ADDRESS, INVOICE DATE, QUANTITY AND DESCRIPTION OF GOOD(S) OR SERVICE(S) FOR WHICH PAYMENT IS BEING REQUESTED, REMITTANCE ADDRESS, AND CONTACT PERSON NAME AND PHONE NUMBER IF THERE IS A PROBLEM WITH THE INVOICE. INVOICES FOR QUANTITIES OR AMOUNTS GREATER THAN WHAT IS STATED ON THE PURCHASE ORDER WILL BE REJECTED. FAILURE TO FOLLOW THESE INSTRUCTIONS MAY RESULT IN DELAYS IN PAYMENT. (aribasystem, Wed, 27 Jan, 2010)
- COMMENT by **Ariba System** on *Wednesday, January 27, 2010 at 11:53 AM*
  The Commodity Group Manager for this purchase is Annie Watkins (aribasystem, Wed, 27 Jan, 2010)

D

District of Columbia Order No : PO494686-V2 –FY14-FA0[redacted] Training-[redacted] (Apr. 17, 2014); District of Columbia Order No : PO494200 –FY14-FA0-Maintenance for [redacted] (Apr. 2, 2014)

Order No : PO494686-V2 -FY14-FA0-[redacted] Training-[redacted]

Issued on Thu, 17 Apr, 2014

Supplier:
HARRIS CORPORATION
1025 W. NASA BLVD.
MELBOURNE, FL 32919
United States
Phone: 1321.727.5391
Fax: 1321.727.5677
Contact: [redacted]

Ship To:
Metropolitan Police Department
300 Indiana Ave. NW Rm 5020
Washington, DC 20001
United States

Bill To:
Metropolitan Police Department
300 Indiana Avenue, NW Rm 4106
Washington, DC 20001
United States
Phone: 1(202) 727-5298

Deliver To:
[redacted]

Bill To Contact: [redacted]
If used in conjunction with a contract award, purchase order is placed in accordance with all provisions of Contract Number: N/A
Requester: [redacted]
Delivery Date: Fri, 18 Apr, 2014
PR No.: RQ853391-V2

Item	Action	Description	Part Number	Unit	Qty	Need By	Unit Price	Extended Amount
1	Modified	[redacted] **Training- to be provided at MPD ...**	[redacted]	each	[redacted]	Fri, 18 Apr, 2014	[redacted] USD	[redacted]
		[redacted] Training- to be provided at MPD facility during the month of June 2014						

Item	Action	Description	Part Number	Unit	Qty	Need By	Unit Price	Extended Amount
2	Modified	[redacted] **Training - to be provided at MPD ...**	[redacted]	each	[redacted]	Fri, 18 Apr, 2014	[redacted] USD	$[redacted] USD
		[redacted] Training - to be provided at MPD facility during the month of June 2014						

Total	$16,000.00 USD

Changes

- Line Item 1, Accounting, Accounting 1, Unpaid Balance changed from [redacted] to (no value)
- Line Item 2, Accounting, Accounting 1, Unpaid Balance changed from [redacted] to (no value)
- ERP Order Comments changed from (no value) to Revised Delivery Date: June 15, 2014

Refer to quote number QTE6779-04809

- ERP Order Comments changed from (no value) to Harris is providing training at the customer¿s facility in Washington DC at the agreed-to price o[redacted] via the referenced quote.
- ERP Order Comments changed from ALL INVOICES SHALL BE SUBMITTED TO THE 'BILL TO' ADDRESS INDICATED ON THIS PURCHASE ORDER. INVOICES SHALL INCLUDE THE PURCHASE ORDER NUMBER, CONTRACT NUMBER (IF APPLICABLE), CONTRACTOR'S NAME AND ADDRESS, INVOICE DATE, QUANTITY AND DESCRIPTION OF GOOD(S) to (no value)
- ERP Order Comments changed from FOB is Destination unless specified otherwise to (no value)
- ERP Order Comments changed from ****GOVERNMENT OF THE DISTRICT OF COLUMBIA STANDARD CONTRACT PROVISIONS FOR USE WITH THE DISTRICT OF COLUMBIA GOVERNMENT SUPPLY AND SERVICES CONTRACTS (July 2010) ARE HEREBY INCORPORATED BY REFERENCE. WWW.OCP.DC.GOV***** to (no value)
- ERP Order Comments changed from The Commodity Group Manager for this purchase is[redacted] to (no value)
- ERP Order Title changed from FY14-FA0-[redacted] Training to FY14-FA0-[redacted] System Training-[redacted]
- Line Item 1, Accounting, Accounting 1, EffectiveDateString changed from 04/10/2014 to 04/07/2014
- Line Item 1, Description, Full Description changed from[redacted] Training to[redacted] Training- to be provided at MPD facility during the month of June 2014
- Line Item 2, Accounting, Accounting 1, EffectiveDateString changed from 04/10/2014 to 04/07/2014
- Line Item 2, Description, Full Description changed from[redacted] Training to[redacted] Training - to be provided at MPD facility during the month of June 2014
- ERP Order TimeCreated changed from Thu, 10 Apr, 2014 to Thu, 17 Apr, 2014

Comments

- [redacted], 04/10/2014:
  Revised Delivery Date: June 15, 2014

  Refer to quote number QTE6779-04809[redacted] Thu, 10 Apr, 2014)
- COMMENT by[redacted] on *04/17/2014*
  Harris is providing training at the customer¿s facility in Washington DC at the agreed-to price of[redacted] via the referenced quote.[redacted] Thu, 17 Apr, 2014)
- COMMENT by **aribasystem** on *04/17/2014*
  ****GOVERNMENT OF THE DISTRICT OF COLUMBIA STANDARD CONTRACT PROVISIONS FOR USE WITH THE DISTRICT OF COLUMBIA GOVERNMENT SUPPLY AND SERVICES CONTRACTS (July 2010) ARE HEREBY INCORPORATED BY REFERENCE. WWW.OCP.DC.GOV***** (ar basystem, Thu, 17 Apr, 2014)
- COMMENT by **aribasystem** on *04/17/2014*
  The Commodity Group Manager for this purchase is[redacted] Thu, 17 Apr, 2014)
- COMMENT by[redacted] on *04/17/2014*
  FOB is Destination unless specified otherwise[redacted] Thu, 17 Apr, 2014)
- COMMENT by **aribasystem** on *04/17/2014*
  ALL INVOICES SHALL BE SUBMITTED TO THE 'BILL TO' ADDRESS INDICATED ON THIS PURCHASE ORDER. INVOICES SHALL INCLUDE THE PURCHASE ORDER NUMBER, CONTRACT NUMBER (IF APPLICABLE), CONTRACTOR'S NAME AND ADDRESS, INVOICE DATE, QUANTITY AND DESCRIPTION OF GOOD(S) OR SERVICE(S) FOR WHICH PAYMENT IS BEING REQUESTED, REMITTANCE ADDRESS, AND CONTACT PERSON NAME AND PHONE NUMBER IF THERE IS A PROBLEM WITH THE INVOICE. INVOICES FOR QUANTITIES OR AMOUNTS GREATER THAN WHAT IS STATED ON THE PURCHASE ORDER WILL BE REJECTED. FAILURE TO FOLLOW THESE INSTRUCTIONS MAY RESULT IN DELAYS IN PAYMENT. (aribasystem, Thu, 17 Apr, 2014)

[redacted]

Order No : PO494200 -FY14-FA0-Maintenance for [redacted]

Issued on Wed, 02 Apr, 2014

Supplier:
HARRIS CORPORATION
1025 W. NASA BLVD.
MELBOURNE, FL 32919
United States
Phone: 1321.727.5391
Fax: 1321.727.5677
Contact: [redacted]

Ship To:
Metropolitan Police Department
300 Indiana Ave. NW Rm 5020
Washington, DC 20001
United States

Bill To:
Metropolitan Police Department
300 Indiana Avenue, NW Rm 4106
Washington, DC 20001
United States
Phone: 1(202) 727-5298

Deliver To:
Lt. Christopher Kauffman

Bill To Contact: [redacted]
If used in conjunction with a contract award, purchase order is placed in accordance with all provisions of Contract Number: [redacted]
Requester: [redacted]
Delivery Date: Fri, 11 Apr, 2014
PR No.: RQ852418

Item	Description	Part Number	Unit	Qty	Need By	Unit Price	Extended Amount
1	[redacted]	[redacted]	each	[redacted]	Fri, 11 Apr, 2014	[redacted] USD	[redacted] USD

Item	Description	Part Number	Unit	Qty	Need By	Unit Price	Extended Amount
2	[redacted]	[redacted]	each	[redacted]	Fri, 11 Apr, 2014	[redacted] USD	[redacted] USD

Item	Description	Part Number	Unit	Qty	Need By	Unit Price	Extended Amount
3	[redacted]	[redacted]	each	[redacted]	Fri, 11 Apr, 2014	[redacted] USD	[redacted] USD

	Total	$8,614.00 USD

Comments

- COMMENT by **aribasystem** on *04/02/2014*
  The Commodity Group Manager for this purchase is [redacted] (aribasystem, Wed, 02 Apr, 2014)
- COMMENT by **aribasystem** on *04/02/2014*
  FOB is Destination unless specified otherwise (aribasystem, Wed, 02 Apr, 2014)
- COMMENT by **aribasystem** on *04/02/2014*
  ****GOVERNMENT OF THE DISTRICT OF COLUMBIA STANDARD CONTRACT PROVISIONS FOR USE WITH THE DISTRICT OF COLUMBIA GOVERNMENT SUPPLY AND SERVICES CONTRACTS (July 2010) ARE HEREBY INCORPORATED BY REFERENCE. WWW.OCP.DC.GOV***** (ar basystem, Wed, 02 Apr, 2014)
- COMMENT by **aribasystem** on *04/02/2014*
  ALL INVOICES SHALL BE SUBMITTED TO THE 'BILL TO' ADDRESS INDICATED ON THIS PURCHASE ORDER. INVOICES SHALL INCLUDE THE PURCHASE ORDER NUMBER, CONTRACT NUMBER (IF APPLICABLE), CONTRACTOR'S NAME AND ADDRESS, INVOICE DATE, QUANTITY AND DESCRIPTION OF GOOD(S) OR SERVICE(S) FOR WHICH PAYMENT IS BEING REQUESTED, REMITTANCE ADDRESS, AND CONTACT PERSON NAME AND PHONE NUMBER IF THERE IS A PROBLEM WITH THE INVOICE. INVOICES FOR QUANTITIES OR AMOUNTS GREATER THAN WHAT IS STATED ON THE PURCHASE ORDER WILL BE REJECTED. FAILURE TO FOLLOW THESE INSTRUCTIONS MAY RESULT IN DELAYS IN PAYMENT. (aribasystem, Wed, 02 Apr, 2014)

E

District of Columbia Order No : PO287717 –[redacted] 2009- Grant fundeed [sic] (Jan. 29, 2009)

Order No : PO287717 - [redacted] 2009- Grant fundeed

Issued on Thu, 29 Jan, 2009

Supplier:
HARRIS CORPORATION
1025 W. NASA BLVD.
MELBOURNE, FL 32919
United States
Phone: 1321.727.6391
Fax: 1321.727.5677
Contact: KEVIN SHAW

Ship To:
Metropolitan Police Department
300 Indiana Ave. NW Rm 5080
Washington, DC 20001
United States

Bill To:
Metropolitan Police Department
300 Indiana Avenue, NW Rm 4106
Washington, DC 20001
United States
Phone: 1(202) 727-5298

Deliver To:
Brian Bray

Item	Description	Part Number	Unit	Qty	Need By	Unit Price	Extended Amount
1	[redacted]		each	3	Fri, 06 Feb, 2009	[redacted] USD	[redacted] USD

Requisition is for 35 hours of [redacted] for three (3) members of the Metropolitan Police Department. The training course will cover the operation and maintenance of [redacted] as well as the procedures for obtaining court orders and subpoenas related to the initiation of [redacted] The course will be held at the Metropolitan Police Academy during the week of February 9th, 2009, through February 13th, 2009. Harris Industries will provide a certified [redacted] as well as training manuals and equipment for class instruction.

If used in conjunction with a contract award, purchase order is placed in accordance with all provisions of Contract Number: N/A
Bill To Contact: [redacted]
Requester: Brian Bray
Form:
Delivery Date: Fri, 6 Feb, 2009
PR No.: RQ524887

Total [redacted] USD

Comments

- APPROVED by [redacted] on *Thursday, January 29, 2009 at 4:21 PM* with comment (1 document attached)
  This requisition has been processed in accordance with applicable laws, regulations and policies/procedures and is ready for approval.

  Contractor shall provid[redacted]in accordance with the Contractor's attached quote, dated 11-25-08, which is hereby incorporated and made part of the purchase order. The training shall be held during the week of February 9, through February 13, 2009. (Reid, Linda, Thu, 29 Jan, 2009)
- COMMENT by **Ariba System** on *Thursday, January 29, 2009 at 4:32 PM*
  FOB is Destination unless specified otherwise (Ariba System, Thu, 29 Jan, 2009)
- COMMENT by **Ariba System** on *Thursday, January 29, 2009 at 4:32 PM*
  *****GOVERNMENT OF THE DISTRICT OF COLUMBIA STANDARD CONTRACT PROVISIONS FOR USE WITH THE DISTRICT OF COLUMBIA GOVERNMENT SUPPLY AND SERVICES CONTRACTS ARE HEREBY INCORPORATED BY REFERENCE, WWW.OCP.DC.GOV***** (Ariba System, Thu, 29 Jan, 2009)
- COMMENT by **Ariba System** on *Thursday, January 29, 2009 at 4:32 PM*
  ALL INVOICES SHALL BE SUBMITTED TO THE 'BILL TO' ADDRESS INDICATED ON THIS PURCHASE ORDER. INVOICES SHALL INCLUDE THE PURCHASE ORDER NUMBER, CONTRACT NUMBER (IF APPLICABLE), CONTRACTOR'S NAME AND ADDRESS, INVOICE DATE, QUANTITY AND DESCRIPTION OF GOOD(S) OR SERVICE(S) FOR WHICH PAYMENT IS BEING REQUESTED, REMITTANCE ADDRESS, AND CONTACT PERSON NAME AND PHONE NUMBER IF THERE IS A PROBLEM WITH THE INVOICE. INVOICES FOR QUANTITIES OR AMOUNTS GREATER THAN WHAT IS STATED ON THE PURCHASE ORDER WILL BE REJECTED. FAILURE TO FOLLOW THESE INSTRUCTIONS MAY RESULT IN DELAYS IN PAYMENT. (Ariba System, Thu, 29 Jan, 2009)
- COMMENT by **Ariba System** on *Thursday, January 29, 2009 at 4:32 PM*
  The Commodity Group Manager for this purchase is Annie Watkins (Ariba System, Thu, 29 Jan, 2009)

F

Re: Acquisition of Wireless Collection Equipment/Technology and Non-Disclosure Obligations (Aug. 17, 2012)

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D.C. 20535-0001

August 17, 2012

Peter Newsham
Assistant Chief
Metro DC Police Department
300 Indiana Ave. NW, #3132
Washington, DC 20001

Re: Acquisition of Wireless Collection Equipment/Technology and Non-Disclosure Obligations

LAW ENFORCEMENT SENSITIVE (LES): The information in this document is the property of the Federal Bureau of Investigation (FBI) and may be distributed within the Federal Government (and its contractors), U.S. intelligence, law enforcement, public safety or protection officials and individuals with a need to know. Distribution beyond these entities without FBI Operational Technology Division authorization is prohibited. Precautions should be taken to ensure this information is stored and/or destroyed in a manner that precludes unauthorized access. Information bearing the LES caveat may not be used in legal proceedings without first receiving authorization from the originating agency. Recipients are prohibited from subsequently posting the information marked LES on a website on an unclassified network.

Dear Assistant Chief Newsham:

We have been advised by Harris Corporation of the Metro DC Police Department's request for acquisition of certain wireless collection equipment/technology manufactured by Harris Corporation. Consistent with the conditions on the equipment authorization granted to Harris Corporation by the Federal Communications Commission (FCC), state and local law enforcement agencies must coordinate with the Federal Bureau of Investigation (FBI) to complete this non-disclosure agreement prior to the acquisition and use of the equipment/technology authorized by the FCC authorization.

As you are aware, law enforcement agencies increasingly rely on wireless collection equipment/technology to conduct lawfully-authorized electronic surveillance. Disclosing the existence of and the capabilities provided by such equipment/technology to the public would reveal sensitive technological capabilities possessed by the law enforcement community and may allow individuals who are the subject of investigation wherein this equipment/technology is used to employ countermeasures to avoid detection by law enforcement. This would not only potentially endanger the lives and physical safety of law enforcement officers and other individuals, but also adversely impact criminal and national security investigations. That is,

disclosure of this information could result in the FBI's inability to protect the public from terrorism and other criminal activity because, through public disclosures, this technology has been rendered essentially useless for future investigations. In order to ensure that such wireless collection equipment/technology continues to be available for use by the law enforcement community, the equipment/technology and any information related to its functions, operation, and use shall be protected from potential compromise by precluding disclosure of this information to the public in any manner including but not limited to: in press releases, in court documents, during judicial hearings, or during other public forums or proceedings. Accordingly, the Metro DC Police Department agrees to the following conditions in connection with its acquisition and use of the Harris Corporation equipment/technology:

1. By entering into this agreement, the Metro DC Police Department affirms that it has statutory authority to lawfully employ this technology and will do so only in support of public safety operations or criminal investigations.

2. The Metro DC Police Department assumes responsibility for operating the equipment/technology in accordance with Federal law and regulation and accepts sole liability for any violations thereof, irrespective of the Federal Bureau of Investigation approval, if any, for the sale of the equipment/technology.

3. The Metro DC Police Department will ensure that operators of the equipment have met the operator training standards identified by the FBI and are certified to conduct operations.

4. The Metro DC Police Department will coordinate with the FBI in advance of its use of the wireless collection equipment/technology to ensure de-confliction of respective missions.

5. The Metro DC Police Department will not distribute, disseminate, or otherwise disclose any information concerning the wireless collection equipment/technology or any software, operating manuals, or related technical documentation (including its technical/engineering description(s) and capabilities) to the public, including to any non-law enforcement individuals or agencies.

6. The Metro DC Police Department will not distribute, disseminate, or otherwise disclose any information concerning the wireless collection equipment/technology or any software, operating manuals, or related technical documentation (including its technical/engineering description(s) and capabilities) provided to it to any other law enforcement or government agency without the prior written approval of the FBI. Prior to any approved distribution, dissemination, or comparable disclosure of any information concerning the wireless collection equipment/technology or any software, manuals, or related technical documentation related to such equipment/technology, all materials shall be marked "Law Enforcement Sensitive, For Official Use Only - Not to be Disclosed Outside of the Metro DC Police Department ."

7. The Metro DC Police Department shall not, in any civil or criminal proceeding, use or provide any information concerning the Harris Corporation wireless collection equipment/technology, its associated software, operating manuals, and any related documentation (including its technical/engineering description(s) and capabilities) beyond the evidentiary results obtained through the use of the equipment/technology including, but not limited to, during pre-trial matters, in search warrants and related affidavits, in discovery, in response to court ordered disclosure, in other affidavits, in grand jury hearings, in the State's case-in-chief, rebuttal, or on appeal, or in testimony in any phase of civil or criminal trial, without the prior written approval of the FBI. If the Metro DC Police Department learns that a District Attorney, prosecutor, or a court is considering or intends to use or provide any information concerning the Harris Corporation wireless collection equipment/technology, its associated software, operating manuals, and any related documentation (including its technical/engineering description(s) and capabilities) beyond the evidentiary results obtained through the use of the equipment/technology in a manner that will cause law enforcement sensitive information relating to the technology to be made known to the public, the Metro DC Police Department will immediately notify the FBI in order to allow sufficient time for the FBI to intervene to protect the equipment/technology and information from disclosure and potential compromise.

   Notification shall be directed to the attention of:

[redacted]
Federal Bureau of Investigation
[redacted]

and

[redacted]
Federal Bureau of Investigation
[redacted]

8. In addition, the Metro DC Police Department will, at the request of the FBI, seek dismissal of the case in lieu of using or providing, or allowing others to use or provide, any information concerning the Harris Corporation wireless collection equipment/technology, its associated software, operating manuals, and any related documentation (beyond the evidentiary results obtained through the use of the equipment/technology), if using or providing such information would potentially or actually compromise the equipment/technology. This point supposes that the agency has some control or influence over the prosecutorial process. Where such is not the case, or is limited so as to be inconsequential, it is the FBI's expectation that the law enforcement

agency identify the applicable prosecuting agency, or agencies, for inclusion in this agreement.

9. A copy of any court order in any proceeding in which the Metro DC Police Department is a party directing disclosure of information concerning the Harris Corporation equipment/technology and any associated software, operating manuals, or related documentation (including its technical/engineering description(s) and capabilities) will immediately be provided to the FBI in order to allow sufficient time for the FBI to intervene to protect the equipment/technology and information from disclosure and potential compromise. Any such court orders shall be directed to the attention of:

[redacted]
Federal Bureau of Investigation
[redacted]

and

[redacted]
Federal Bureau of Investigation
[redacted]

10. The Metro DC Police Department will not publicize its acquisition or use of the Harris Corporation equipment/technology or any of the capabilities afforded by such equipment/technology to the public, other law enforcement agencies, or other government agencies, including, but not limited to, in any news or press releases, interviews, or direct or indirect statements to the media.

11. In the event that the Metro DC Police Department receives a request pursuant to the Freedom of Information Act (5 U.S.C. § 552) or an equivalent state or local law, the civil or criminal discovery process, or other judicial, legislative, or administrative process, to disclose information concerning the Harris Corporation wireless collection equipment/technology, its associated software, operating manuals, and any related documentation (including its technical/engineering description(s) and capabilities), the Metro DC Police Department will immediately notify the FBI of any such request telephonically and in writing in order to allow sufficient time for the FBI to seek to prevent disclosure through appropriate channels. Notification shall be directed to the attention of:

[redacted]
Federal Bureau of Investigation
[redacted]

and

[redacted]
Federal Bureau of Investigation
[redacted]

The Metro DC Police Department's acceptance of the above conditions shall be evidenced by the signatures below of an authorized representative and wireless collection equipment operators of the Metro DC Police Department.

Sincerely,

[redacted]

Federal Bureau of Investigation

Acknowledged and agreed to this _____ day of _____, 2012.

[redacted]

Paul Newsham
Assistant Chief
Metro DC Police Department
[redacted]

[redacted]

G

Application, *In re Application of the State of Maryland for an Order Authorizing the Installation and Use of a Device Known as a Pen Register/Trap & Trace Over 443-208-2776* (Cir. Ct. for Balt. City, Md., May 5, 2014)

IN THE MATTER OF AN APPLICATION	*	**IN THE**
OF THE STATE OF MARYLAND	*	**CIRCUIT COURT**
FOR AN ORDER AUTHORIZING THE	*	**FOR**
INSTALLATION AND USE OF A DEVICE	*	**BALTIMORE CITY**
KNOWN AS A PEN REGISTER /	*	**STATE**
TRAP & TRACE	*	**OF MARYLAND**
OVER	*	
443-208-2776	*	

* * * * * * * * *

APPLICATION

Your Applicant, Detective Michael Spinnato, Baltimore Police Department, pursuant to section 10-4B-03 of the Courts Article of the Code of Maryland, hereby applies for an Order authorizing the installation and use of a device known as a Pen Register \ Trap & Trace and Cellular Tracking Device to include cell site information, call detail, without geographical limits, which registers telephone numbers dialed or pulsed from or to the telephone(s) having the number(s): 443-208-2776 , a AT&T; Sprint / Nextel; Virgin Mobile; T-Mobile; Cellco Partnership, DBA Verizon Wireless; Cricket Communications, Inc; and / or any other Telecommunication service provider telephone.

In support of this application, your applicant states as follows:

Your applicant, Detective Michael Spinnato , Baltimore Police Department ("Agency"), has been engaged in an investigation of Kerron Andrews for violation of Attempted

Murder. The following information is offered in support of probable cause for the interception of real-time cell site information.

1. On 4/27/14 members of the Baltimore City Police Department investigated a Shooting that occurred at 4900 Stafford St under complaint number 148D12125

2. During the course of the investigation a suspect was developed and identified as "Kerron Andrews" M/B 5/19/1991.

3. Investigators subsequently obtained an arrest warrant for the suspect on 5/2/2014 charging him with Attempted Murder and related charges. (2B02259343,D140312104)

4. Det. Spinnato conducted a background investigation and found several possible addresses where the suspect may be living. These locations were turned up with negative results at this time.

5. Investigators were able to obtain Mr. Andrews cell phone number 443-208-2776, thru the victims cell phone records. Further investigation revealed that Mr. Andrews is a confidential informant and that his point of contact within the department is a Det. Lugo. Your writer contacted Det. Lugo who confirmed that Mr. Andrews cell phone number is 443-208-2776.

6. In order to hide from police, investigators know suspects will contact family, girlfriends, and other acquaintances to assist in their day to day covert affairs. Detective Spinnato would like to track/monitor Mr. Andrews' cell phone activity to further the investigation an assist in Mr. Andrews' apprehension.

7. Therefore, your applicant respectfully requests this court order to assist in the apprehension of this suspect. Mr. Andrews is aware of his warrant and is actively eluding law enforcement officials. Based on your affiant's training and experience, it is known that suspects typically use cellular phones until service is terminated or the phone becomes non-functional.

2. Your Applicant hereby certifies that the information likely to be obtained concerning the aforesaid individual's location will be obtained by learning the numbers, locations and subscribers of the telephone number(s) being dialed or pulsed from or to the aforesaid telephone and that such information is relevant to the ongoing criminal investigation being conducted by the Agency.

WHEREFORE, the State of Maryland respectfully requests that this Court grant an Order:

A. Authorizing the Agency to install and use a Pen Register \ Trap & Trace and Cellular Tracking Device to include cell site information, call detail, without geographical limits upon the aforesaid telephone(s) for a period of time not to exceed sixty (60) days.

B. Directing that the Agencies shall complete the necessary installation of the Pen Register \ Trap & Trace and Cellular Tracking Device, utilizing AT&T; Sprint / Nextel; Virgin Mobile; T-Mobile; Cellco Partnership, DBA Verizon Wireless, Verizon; Cricket Communications, Inc; and / or any other Telecommunication service provider providing service for the

above listed target phone number, facilities, technical information and equipment, if required.

C. Directing that if requested by the agencies, AT&T; Sprint / Nextel; Virgin Mobile; T-Mobile; Cellco Partnership, DBA Verizon Wireless, Verizon; Cricket Communications, Inc; and / or any other Telecommunication service provider, direct the target telephone number to operate according to the Global System for Mobile Communications (GSM), Code Division Multiple Access (CDMA) , or Integrated Digital Enhanced Network (iDEN) protocols as applicable.

D. Directing that if requested by the agencies, T-Mobile and/or AT&T direct the target telephone number to operate according to the Global System for Mobile Communications (GSM) protocols.

E. Directing that the Agencies are authorized to employ surreptitious or duplication of facilities, technical devices or equipment to accomplish the installation and use of a Pen Register \ Trap &Trace and Cellular Tracking Device, unobtrusively and with a minimum of interference to the service of the subscriber(s) of the aforesaid telephone, and 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), Reveal Reports, PCMD (Per Call Measurement Data) Report, Precision Locations and any

and all locations, and such provider 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 and at such intervals and times as directed by the law enforcement agent / agencies serving the Order.

F. Directing that there are specific and articulate facts that AT&T; Sprint / Nextel; Virgin Mobile; T-Mobile; Cellco Partnership, DBA Verizon Wireless, Verizon; Cricket Communications, Inc; and / or any other Telecommunication service provider providing service for the above listed target phone number, shall furnish the Agencies with all information, facilities, cell site locations with sector information, any and all equipment information including (but not limited to) mobile station identification (MSID), international mobile subscriber identifier (IMSI), electronic serial number (ESN), subscriber identity module (SIM), international mobile equipment identity (IMEI) and other equipment identifying number(s), subscriber and billing information including (but not limited to) the amount of money/minutes on prepaid phones, account information including (but not limited to) customer comments, remarks, customer billing and warranty information, or any other customer contact notations and other phone number[s] on the account, call history records, and technical assistance necessary to accomplish the installation and use of a Pen Register \ Trap & Trace and Cellular Tracking Device, unobtrusively

and with a minimum of interference to the service of the subscriber(s) of the aforesaid telephone, Global Position System Tracing and Tracking, Mobile Locator tools, R.T.T. (Real Time Tracking Tool), Precision Locations and any and all locations.

G. Directing AT&T; Sprint / Nextel; Virgin Mobile; T-Mobile; Cellco Partnership, DBA Verizon Wireless, Verizon; Cricket Communications, Inc; and / or any other Telecommunication service provider to provide twenty-four (24) hour technical support and implementation assistance.

H. Directing AT&T; Sprint / Nextel; Virgin Mobile; T-Mobile; Cellco Partnership, DBA Verizon Wireless, Verizon; Cricket Communications, Inc; and / or any other Telecommunication service provider to provide any and all historical billing and subscriber information listed to this number and line, and / or any number(s) and line(s) that this target number has been changed to within ten (10) days prior to the implementation of this order.

I. Directing the Agency to compensate AT&T; Sprint / Nextel; Virgin Mobile; T-Mobile; Cellco Partnership, DBA Verizon Wireless, Verizon; Cricket Communications, Inc; and / or any other Telecommunication service provider for reasonable expenses for the services, which the Company is providing.

J. Directing AT&T; Sprint / Nextel; Virgin Mobile; T-Mobile; Cellco Partnership, DBA Verizon Wireless, Verizon; Cricket Communications,

Inc; and / or any other Telecommunication service provider shall continue to provide the Agencies subscriber information of telephone numbers dialed from or to the aforesaid telephone, provided such request is made within ten (10) days of the expiration of the Order and provide up to 365 days of prior detailed call history information (to include SMS and MMS), of the aforesaid target telephone, only if requested by the Agency.

K. Directing that Verizon of Maryland, Inc., Comcast, Cavalier, AT&T; Sprint / Nextel; Virgin Mobile; T-Mobile; Cellco Partnership, DBA Verizon Wireless, Verizon; Cricket Communications, Inc; and / or any other Telecommunication service provider shall provide the Agencies with subscriber information of published and non-published telephone numbers obtained from the aforesaid telephone, provided that the request for such information is made within ten (10) days of the expiration of the Order.

L. Directing that AT&T; Sprint / Nextel; Virgin Mobile; T-Mobile; Cellco Partnership, DBA Verizon Wireless, Verizon; Cricket Communications, Inc; and / or any other Telecommunication service provider and its agents and employees are prohibited from disclosing to the subscriber(s) of the aforesaid telephone(s) or to any other person(s) the existence of this Application and Order, the existence of the investigation identified in the Application or the fact that the Pen Register \ Trap & Trace and Cellular Tracking Device to include cell site information, call detail, without geographical limits, is being installed and used upon the aforesaid

telephone(s).

M. Directing that the Order authorizing the installation and use of the devices apply not only to the presently assigned number(s) and line(s), but to any subsequent number(s), line(s) or service(s) assigned to replace the original number(s) or line(s); and that any change to the service(s), additional services, leased or purchased equipment, enhanced and/or special or custom feature(s), changing of mobile station identification (MSID), international mobile subscriber identifier (IMSI), electronic serial number (ESN), subscriber identity module (SIM), or international mobile equipment identity (IMEI) be disclosed to the Applicants.

N. Directing that during the effective period of the Order, AT&T; Sprint / Nextel; Virgin Mobile; T-Mobile; Cellco Partnership, DBA Verizon Wireless, Verizon; Cricket Communications, Inc; and / or any other Telecommunication service provider, shall not discontinue, suspend, or change the provision of service to the above-described telephone(s) for any reason, including but not limited to suspicion of fraud, or non-payment of outstanding bills without first providing notice to the Agencies, via the Baltimore Police Department at 443-984-7266 and without further providing the Agencies with the opportunity to assume the cost of any unpaid services provided by AT&T; Sprint / Nextel; Virgin Mobile; T-Mobile; Cellco Partnership, DBA Verizon Wireless, Verizon; Cricket Communications, Inc; and / or any other Telecommunication

service provider. Directing the Agencies shall pay the cost of any unpaid services provided by AT&T; Sprint / Nextel; Virgin Mobile; T-Mobile; Cellco Partnership, DBA Verizon Wireless, Verizon; Cricket Communications, Inc; and / or any other Telecommunication service provider with respect to the above-described telephone(s), from the date AT&T; Sprint / Nextel; Virgin Mobile; T-Mobile; Cellco Partnership, DBA Verizon Wireless, Verizon; Cricket Communications, Inc; and / or any other Telecommunication service provider notifies the Agencies of its intention to discontinue, suspend or change the provision of service(s) to the phone(s), up until the date that the Agencies advises AT&T; Sprint / Nextel; Virgin Mobile; T-Mobile; Cellco Partnership, DBA Verizon Wireless, Verizon; Cricket Communications, Inc; and / or any other Telecommunication service provider that it will not or will no longer assume and pay the cost of continued unpaid service(s).

O. Directing AT&T; Sprint / Nextel; Virgin Mobile; T-Mobile; Cellco Partnership, DBA Verizon Wireless, Verizon; Cricket Communications, Inc; and / or any other Telecommunication service provider will not sell or transfer the telephone number(s) or facility(ies) without prior notice to the Agency.

P. Directing that AT&T; Sprint / Nextel; Virgin Mobile; T-Mobile; Cellco Partnership, DBA Verizon Wireless, Verizon; Cricket Communications, Inc; and / or any other Telecommunication service provider provide the

Agency with identical services to those received by the subscriber(s), including all communications transmitted over the telephone(s) that the subscriber(s) receive(s), regardless of which other communications common carrier'(s) facilities are involved.

Q. Directing that AT&T; Sprint / Nextel; Virgin Mobile; T-Mobile; Cellco Partnership, DBA Verizon Wireless, Verizon; Cricket Communications, Inc; and / or any other Telecommunication service provider provide the Agency with all call data content, transactional/call, data/call detail and cell site data simultaneous with all communications over 443-208-2776.

R. Directing that this Application and Order be sealed.

Respectfully submitted,

Detective Michael Spinnato,
Baltimore Police Department

Upon a finding that probable cause exists based upon the information supplied in this application, that the said individual is using the cellular phone number of 443-208-2776 for criminal activity and that the application will lead to evidence of the crime(s) under the investigation.

Sworn and Subscribed to before me this 5 of May, 2014.

Judge Barry G. Williams
Circuit Court for Baltimore City
Signature appears on the original document

Judge
Circuit Court for Baltimore City

TRUE COPY
TEST

FRANK M. CONAWAY, CLERK

CIRCUIT COURT FOR BALTIMORE CITY
1983

H

Def's Mot. to Compel Disclosure of Evidence, *State v. Thomas*, No. 2008-CF-3350 (Fla. 2d Cir. Ct. Aug. 2, 2010)

IN THE CIRCUIT COURT OF THE SECOND JUDICIAL CIRCUIT
IN AND FOR LEON COUNTY, FLORIDA.

STATE OF FLORIDA

vs.

JAMES THOMAS,
Defendant.
_____/

CASE NO. 08CF03350
Division "C"
Spn. 175470

DEFENDANT'S MOTION TO COMPEL DISCLOSURE OF EVIDENCE

Defendant, James Thomas, through his undersigned attorney, moves this Court to compel the disclosure of certain evidence and in support of this motion says:

1. The particular evidence sought to be disclosed are the "covert investigative techniques" utilized by Investigator Christopher Corbitt to locate the cell phone of C.M., which ultimately lead law enforcement to Defendant's residence, statements made by Defendant to law enforcement and Defendant's arrest in the above-styled case.

2. During his deposition, Investigator Corbitt refused to disclose those techniques. Attached are pages six through eight of his deposition, which discusses Investigator Corbitt's unwillingness to disclose the techniques.

3. Defendant is entitled to disclosure of those techniques pursuant to the discovery provisions of the Florida Rules of Criminal Procedure and the due process provisions of the Florida and United States Constitutions. Defendant does not concede the lawfulness or appropriateness of using those techniques, and is entitled to know them in order to determine the lawfulness of law enforcement's initial contact with him and his residence.

Defendant does not object to such disclosure in camera or under seal in order to protect the integrity of the techniques.

4. Defendant presumes that the State objects to disclosing such evidence.

WHEREFORE, Defendant moves this Court to grant relief consistent with this motion.

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that a true and correct copy of this document has been furnished by hand delivery to the Office of the State Attorney, at the Leon County Courthouse, 301 South Monroe Street, Tallahassee, Florida 32301, this 2nd day of August, 2010.

OFFICE OF CRIMINAL CONFLICT & CIVIL REGIONAL COUNSEL, REGION ONE

Daren L. Shippy
Assistant Regional Counsel
FL Bar ID No. 508810
P.O. Box 1019
Tallahassee, FL 32302
(850) 922-0179
(850) 922-9970 FAX

locate property belonging to the victim.

Q And what kind of property was that?

A There was -- my understanding is there were several items that were missing, including a purse, some personal property, a cell phone, identification, some other items that were missing from her.

Q All right. Is it fair to say that the primary use of the investigating -- investigatory techniques was the cellular phone?

A The cellular phone is a potential target for location, yes.

Q Was that, in fact, the primary use of the techniques in this case?

A In this case, as documented in the report, yes, the cell phone was the primary.

Q All right. Was that, in fact, used to locate -- was the investigatory technique used to locate the cell phone in this case?

A Yes. Covert investigative techniques were used to locate the cell phone.

Q Okay. Now I do have to ask you, Investigator Corbitt, what are those techniques?

A I really can't go into detail. They are covert, Department-approved surveillance techniques, universally accepted, used, trained, specialized.

Q Okay. Now go ahead, I'm sorry.

A That's probably the best that I can say.

Q All right. Now for the record I do have to ask you: Why can't you divulge that information?

A From a confidentiality nature, the techniques that we utilize are done so in an effect to save lives and to serve the citizens. The more that information is revealed and the techniques, the details of that are revealed, then the ability to counter those techniques are made known. So we attempt to keep those techniques, the nature of them, the specific nature, covert so as that they remain effective in their use.

Q Okay. Now you mentioned confidentiality. What specifically -- when you say confidentiality forbids you from discussing these techniques, where is this confidentiality developed from? Is it simply a Department policy, or is this a law that I'm not aware of?

A Well, it is a Department philosophy not to reveal covert surveillance techniques. There is also some protection for surveillance techniques such that, you know, standing case law that I don't have to reveal -- if I'm doing visual surveillance from a home in a neighborhood, I don't have to reveal the specific location of that home, merely that I'm doing visual

surveillance, so --

Q All right. Investigator, did you have any other involvement in this case outside of what we've already talked about?

A I was present in the local area while some of the contact was going on at the apartment. I did begin to take down the legal description of the apartment in anticipation of a search warrant. I made notes as far as the specific legal description.

Q Did you, in fact, go to -- go -- or strike that.

Did you attempt to obtain a search warrant for the apartment?

A Myself, it is not my responsibility to actually obtain the search warrant. To assist the investigators who were going to do that, I did begin documenting the legal description because I was on scene. That description would be relayed to someone who would actually be typing up the search warrant.

Q Okay. So what was your involvement with regard to obtaining a search warrant exactly?

A It was simply obtaining the legal description of the apartment, which is required in the search warrant document; and, additionally, I would be providing some of the probable cause related to the

Certificate of Service

I hereby certify that on February 22, 2015, copies of the foregoing Brief of the American Civil Liberties Union, American Civil Liberties Union of the Nation's Capital, and Electronic Frontier Foundation as Amici Curiae were served by first-class mail and by email upon:

Elizabeth Trosman
Chief, Appellate Division
Office of the United States Attorney
555 Fourth Street, NW
Washington, DC 20530

Stefanie Schneider
Public Defender Service for
the District of Columbia
633 Indiana Avenue, NW
Washington, DC 20004

In addition, a copy in PDF format was sent to the Court by email addressed to briefs@dcappeals.gov.

Arthur B. Spitzer