Linda Lye (CA SBN 215584)
llye@aclunc.org
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF NORTHERN CALIFORNIA
39 Drumm Street, 2nd Floor
San Francisco, California 94111
Telephone: 415-621-2493
Facsimile: 415-255-8437

ATTORNEYS FOR *AMICUS* AMERICAN CIVIL
LIBERTIES UNION OF NORTHERN CALIFORNIA

Ezekiel Edwards (eedwards@aclu.org)
Nathan Freed Wessler (nwessler@aclu.org)
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Telephone: 212-549-2500
Facsimile: 212-549-2654

ATTORNEYS FOR *AMICUS*
AMERICAN CIVIL LIBERTIES UNION

Hanni M. Fakhoury (CA SBN 252629)
hanni@eff.org
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: 415-436-9333
Facsimile: 415-436-9993

ATTORNEYS FOR *AMICUS*
ELECTRONIC FRONTIER FOUNDATION

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. DIAZ-RIVERA, et al., Defendants.	CASE No.: 12-cr-00030-EMC/EDL **BRIEF *AMICI CURIAE* OF ACLU, ACLU OF NORTHERN CALIFORNIA AND ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF DEFENDANTS' MOTION TO COMPEL DISCOVERY** Hearing Date: November 5, 2013 Time: 9:00 a.m. Location: San Courtroom E, 15th Floor

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases **Page(s)**

Statutes

Rules

Congressional Materials

Other Authorities

I. INTRODUCTION

This case likely involves one or more highly controversial surveillance programs: the National Security Agency's Mass Call-Tracking Program and the Hemisphere Project, both of which involve vast databases of Americans' phone records, as well as so-called "stingray" devices, sophisticated tools that mimic a cell tower and thereby scoop up information from wireless devices in the vicinity. *Amici* submit this brief, in support of Defendants' Motion to Compel Discovery, in order to provide important context and to underscore the larger implications of this case.

First, the NSA Mass Call-Tracking Program, the Hemisphere Project, and stingray devices are highly intrusive and unconstitutional. *Second*, due process and Federal Rule of Criminal Procedure 16 require the government to disclose to Defendants information that would allow them to challenge in a motion to suppress unconstitutional forms of electronic surveillance used to further this investigation. *Third*, disclosure of the information sought by Defendants has a wider significance beyond this case. The government shrouds its surveillance practices in secrecy, but that secrecy undermines democratic governance and prevents the federal courts from reviewing the legality of intrusive and unconstitutional forms of surveillance.

II. ARGUMENT

A. The NSA Mass Call-Tracking Program, The Hemisphere Project, And Stingray Devices Are Unconstitutional

1. The National Security Agency's Mass Call-Tracking Program

a. The Federal Government Has Amassed A Vast Database Of Americans' Call Records

On June 5, 2013, *The Guardian* disclosed a previously secret order from the Foreign Intelligence Surveillance Court directing Verizon Business Network Services to produce to the National Security Agency "on an ongoing daily basis . . . all call detail records or 'telephony metadata'" relating to every domestic and international call placed on its network between April

25, 2013 and July 19, 2013; the order specified that telephony metadata include, for each phone call, the originating and terminating telephone number as well as the call's time and duration. [1]

On the day the order expired, the Director of National Intelligence issued a statement indicating that the Foreign Intelligence Surveillance Court had renewed it.[2] The order was issued as part of a broader program that has been in place for seven years and that involves the collection of information about virtually every phone call, domestic and international, made or received in the United States.[3]

The government has utilized its mass call-tracking database in the course of investigations that resulted in criminal prosecutions. For example, the government searched its database when investigating a planned bombing of the New York City subway and then prosecuted the investigative targets. [4] The government also utilized the program in the course of investigating an individual named Basaaly Moalin,[5] who was subsequently convicted of providing material support to a terrorist group.[6]

---

[1] *In re Application of the FBI for an Order Requiring the Production of Tangible Things from Verizon Bus. Network Servs., Inc. on Behalf of MCI Commc'n Servs., Inc. d/b/a Verizon Bus. Servs.*, No. BR 13-80 at 2 (FISA Ct. Apr. 25, 2013)), *available at* http://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order; *see also* Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN (June 5, 2013), *available at* http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order. In the days after *The Guardian* disclosed the Secondary Order, Director of National Intelligence James Clapper acknowledged its authenticity. *See* Press Release, Office of the Director of National Intelligence, DNI Statement on Recent Unauthorized Disclosures of Classified Information (June 6, 2013), *available at* http://1.usa.gov/13jwuFc.

[2] Press Release, Office of the Director of National Intelligence, Foreign Intelligence Surveillance Court Renews Authority to Collect Telephony Metadata (July 19, 2013), *available at* http://1.usa.gov/12ThYlT.

[3] ADMINISTRATION WHITE PAPER: BULK COLLECTION OF TELEPHONY METADATA UNDER SECTION 215 OF THE USA PATRIOT ACT 1 (Aug. 9, 2013), *available at* http://bit.ly/15ebL9k; Dep't of Justice, *Report on the National Security Agency's Bulk Collection Programs for USA PATRIOT Act Reauthorization* 3 (Feb. 2, 2011), *available at* http://1.usa.gov/1cdFJ1G.

[4] *ACLU v. Clapper*, S.D.N.Y. Case No. 13-cv-03994, Defs' Mem. of Law in Opposition to Pls.' Motion for a Preliminary Injunction at10-11, ECF No. 61 (Oct. 1, 2013) (excerpts attached as Lye Decl., Exh. 1).

[5] Oversight of FISA (Foreign Intelligence Surveillance Act) Surveillance Programs: Hearing of the Senate Judiciary Committee on Strengthening Privacy Rights and National Security, 113th Cong. (2013) (oral testimony of Sean Joyce), *available at* http://icontherecord.tumblr.com/post/57811913209/hearing-of-the-senate-judiciary-committee-on ("As you mentioned another

Although the nature and extent of data flows from the NSA to other federal law enforcement agencies is largely secret, it is clear that NSA-derived information is provided to other law enforcement entities. In the New York City subway investigation, the NSA supplied data derived from the mass call-tracking database to the FBI.[7] Also, the Drug Enforcement Administration ("DEA") has institutionalized the dissemination of NSA-derived information to other law enforcement agencies through its Special Operations Division ("SOD").[8] According to *Reuters*, SOD is tasked with "funneling information" from intelligence sources to "authorities across the nation to help them launch criminal investigations of Americans."[9]

Although it is unclear whether information obtained by the NSA's mass call-tracking program is disseminated by the SOD, that lack of clarity is attributable to the DEA's deliberate efforts to conceal the origins of intelligence-derived information. A document obtained by *Reuters* "specifically directs agents to omit the SOD's involvement from investigative reports, affidavits, discussions with prosecutors and courtroom testimony. Agents are instructed to then use 'normal investigative techniques to recreate the information provided by SOD.'"[10]

b. The Warrantless Bulk Collection Of Phone Records Is Unconstitutional

The NSA's warrantless collection of all domestic telephony metadata violates Fourth Amendment privacy rights and First Amendment associational rights.

---

instance when we used the business record 215 program, as Chairman Leahy mentioned, Basaaly Moalin.").

[6] Press Release, Federal Bureau of Investigation, San Diego Division, San Diego Jury Convicts Four Somali Immigrants of Providing Support to Foreign Terrorists (Feb. 22, 2013), *available at* http://www.fbi.gov/sandiego/press-releases/2013/san-diego-jury-convicts-four-somali-immigrants-of-providing-support-to-foreign-terrorists.

[7] *ACLU v. Clapper*, S.D.N.Y. Case No. 13-cv-03994, Defs' Mem. of Law in Opposition to Pls.' Motion for a Preliminary Injunction at10-11, ECF No. 61 (Oct. 1, 2013) ("NSA received [a suspect's] telephone number from the FBI and ran it against the telephony metadata, identifying and passing additional leads back to the FBI for investigation.").

[8] John Shiffman & Kristina Cooke, *U.S. Directs Agents To Cover Up Programs Used To Investigate Americans*, REUTERS (Aug. 5, 2013), *available at* http://www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805.

[9] *Id.*

[10] *Id.*

The program permits the government to assemble a richly detailed profile of every person living in the United States and to draw a comprehensive map of their associations with one another. The long-term recording and aggregation of telephony metadata achieves essentially the same kind of privacy intrusion that led five Justices of the Supreme Court to conclude in *United States v. Jones*, 132 S. Ct. 945 (2012), that the long-term recording and aggregation of location information constituted a search. In *Jones*, the Supreme Court considered whether police had conducted a Fourth Amendment search when they attached a GPS-tracking device to a vehicle and monitored its movements over a period of 28 days. The Court held that the installation of the GPS device and the use of it to monitor the vehicle's movements constituted a search because it involved a trespass "conjoined with . . . an attempt to find something or to obtain information." *Id.* at 951 n.5. In two concurring opinions, five Justices concluded that the surveillance constituted a search because it "impinge[d] on expectations of privacy." *Id.* at 964 (Alito, J., concurring in judgment); *id.* at 955 (Sotomayor, J., concurring). As with the long-term location tracking in *Jones*, the surveillance at issue here "enables the Government to ascertain, more or less at will, [every person's] political and religious beliefs, sexual habits, and so on." *Id.* at 956 (Sotomayor, J., concurring).

The mass call-tracking program also violates the First Amendment. The Supreme Court has recognized that the government's surveillance and investigatory activities can infringe on associational rights protected by the First Amendment. Thus in *NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449 (1958), a case in which the Supreme Court invalidated an Alabama order that would have required the NAACP to disclose its membership lists, the Court wrote, "[i]t is hardly a novel perception that compelled disclosure of affiliation with groups engaged in advocacy" may operate as "a restraint on freedom of association." *Id.* at 462. The government's mass call-tracking program raises precisely the same specter of associational harm by permitting the government to track every one of Defendants' telephone contacts.

//

//

2. The Hemisphere Project

a. The Federal Government Has Amassed Yet Another Vast Database Of Americans' Call Records

In September 2013, the New York Times reported the existence of the Hemisphere Project, a previously hidden program in which the "government pays AT&T to place its employees in drug-fighting units around the country. Those employees sit alongside Drug Enforcement Administration agents and local detectives and supply them with the phone data from as far back as 1987."[11] The report was based on a set of training slides obtained by the Times. *See* Defs' Exh. L (ECF No. 242-1) (hereinafter "Hemisphere Slide Deck").[12]

The Hemisphere Project involves a massive database of call detail records ("CDRs") for every phone call that travels through an AT&T switch, whether placed using AT&T or another telephone carrier. *See id.* at 2. The CDRs in the Hemisphere database include not only information about dialed telephone numbers and other call routing data, but also information about the locations of callers. *See id.* at 3, 13. The database contains CDRs dating from 1987 to the present, and a search of the database will "include CDRs that are less than one hour old at the time of the search." *See id.* at 3. A staggering four billion CDRs are added to the Hemisphere database each day. *See id.* at 2. The government, which funds Hemisphere, obtains CDRs from the database by directing administrative subpoenas at embedded AT&T employees, who then query the system for records and return them in the government's preferred format. *See id.* at 2-3.

"Hemisphere is most often used by DEA and DHS in the Northwest [High Intensity Drug Trafficking Area] to identify replacement/additional phones." *Id.* at 4. The project is

---

[11] Scott Shane & Colin Moynihan, *Drug Agents Use Vast Phone Trove, Eclipsing N.S.A.'s*, N.Y. TIMES (Sept. 1, 2013), *available at* http://www.nytimes.com/2013/09/02/us/drug-agents-use-vast-phone-trove-eclipsing-nsas.html.

[12] The training slides were posted by the New York Times on its website. *See* Office of Nat'l Drug Control Policy, *Los Angeles Hemisphere*, *available at Synopsis of the Hemisphere Project*, N.Y. TIMES (Sept. 1, 2013), http://www.nytimes.com/interactive/2013/09/02/us/hemisphere-project.html.

"coordinated" from California. *Id.* at 2. DEA-funded AT&T employees search the contents of the database of call records using algorithms and other techniques to identify new phones whose calling patterns are similar to a person's old or existing phone; thus when the target of an investigation ceases using one phone and/or acquires an additional one, Hemisphere provides the government with a list of "candidates for the replacement phone . . . ranked by probability." *Id.* at 5-6, 7.

Troublingly, the government has engaged in a systematic campaign to conceal the existence and use of the Hemisphere Project from the public, including from defense attorneys and their clients. Law enforcement agents are "instructed to never refer to Hemisphere in any official document" and to "keep the program under the radar." *Id.* at 8, 12. In cases where agents use Hemisphere to obtain CDRs and identify a suspect's new or additional phone, they are directed to submit a second administrative subpoena to the suspect's carrier (whether AT&T or another provider) for the CDRs related to the new phone number and to make reference only to those records in any public materials, thus "walling off" the Hemisphere Project from disclosure. *Id.* at 10.

b. The Hemisphere Project Is Unconstitutional

Like the NSA mass call-tracking program, Hemisphere violates the Fourth and First Amendments.

The Hemisphere Project is unlike typical government requests to phone companies for CDRs. In run-of-the-mill investigations, the government seeks a judicial order to the phone company and then awaits the results of the company's compliance. *See, e.g.*, *United States v. Ruby*, 2013 WL 544888, at *3 (S.D. Cal. Feb. 12, 2013) (government acquired call detail records from service provider after obtaining and serving order pursuant to 18 U.S.C. § 2703(d)). Here, however, the government funds and directs the entire process by paying AT&T to embed its employees within DEA operational units, directing their search of the Hemisphere system, and then obtaining CDRs in a format requested by the DEA. This constitutes state action, as the government has created an agency relationship with embedded AT&T employees

and has directed their searches of trillions of call records without warrants. *See United States v. Reed*, 15 F.3d 928, 931 (9th Cir. 1994) ("[T]he Fourth Amendment does prohibit unreasonable intrusions by private individuals who are acting as government instruments or agents."). Hemisphere is functionally indistinguishable from mass surveillance programs where the government installs agents and monitoring equipment in phone company facilities and searches incoming or transiting phone traffic. *Cf. Jewel v. Nat'l Sec. Agency*, 673 F.3d 902, 906 (9th Cir. 2011) (holding that plaintiffs have standing to bring Fourth Amendment challenge to NSA surveillance program that diverted all internet traffic passing through AT&T facilities into a "SG3 Secure Room" in those facilities, where "information of interest [was] transmitted from the equipment in the SG3 Secure Rooms to the NSA based on rules programmed by the NSA" (alteration in original) (internal quotation marks omitted)).

At a minimum, Hemisphere raises similar constitutional concerns as the NSA mass call-tracking database. The government is querying the stored call records of millions of people in the United States in order to identify patterns in the communications and associations of a few individuals. But the program sweeps up the records of millions of individuals who are not the subject of any investigation, amassing their call records even though there is no suspicion they have engaged in criminal wrongdoing, and analyzing their records without a warrant, and hence, without any judicial oversight. This violates the Fourth and First Amendments. *Supra* Part II-A-1-b. But Hemisphere goes even further than the NSA's mass call-tracking program, as the CDRs stored in the Hemisphere database contain location information about callers (*see* Hemisphere Slide Deck at 3, 13), thus implicating the specific concerns raised by five Justices in *Jones*. *See* 132 S. Ct. at 955 (Sotomayor, J., concurring) ("wealth of detail about [a person's] familial, political, professional, religious, and sexual associations" revealed through "trips to the psychiatrist, the plastic surgeon, the abortion clinic," etc.) (internal quotation marks, citation omitted); *id.* at 964 (Alito, J., concurring).

Because the existence of the Hemisphere Project had been deliberately kept secret from the Defendants and the public at large until last month, despite use of the program in numerous

drug cases (*see* Hemisphere Slide Deck at 4, 14-26), a suppression motion by Defendants would be the first opportunity of which *amici* are aware for the judiciary to assess the constitutionality of Hemisphere surveillance.

3. Stingrays

a. Stingrays Scoop Up Information From Innocent Third Party Wireless Devices

"Stingray" is the name for the Harris Corporation's line of "cell site simulator" devices, also called "IMSI catchers," in reference to the unique identifier – or international mobile subscriber identity – of wireless devices.[13] Wireless carriers provide coverage through a network of base stations that connect wireless devices on the network to the regular telephone network. An IMSI catcher masquerades as a wireless carrier's base station, prompting wireless devices to communicate with it. Stingrays are commonly used in two ways: to collect unique numeric identifiers associated with phones in a given location or to ascertain the location of a phone "when the officers know the numbers associated with it but don't know precisely where it is."[14] Several features of stingrays are noteworthy.

First, the devices broadcast electronic signals that penetrate the walls of private locations not visible to the naked eye, including homes, offices, and other private locations of the target and third parties in the area.[15]

Second, the devices can pinpoint an individual with extraordinary precision, in some

---

[13] Although "Stingray" refers to a specific line of Harris Corporation products, *see infra* at note 15, *amici* use the term "stingray" in this brief generically to refer to IMSI catchers.

[14] Jennifer Valentino-DeVries, *How 'Stingray' Devices Work*, WALL STREET JOURNAL (Sept. 21, 2011), *available at* http://blogs.wsj.com/digits/2011/09/21/how-stingray-devices-work/.

[15] The devices send signals like those emitted by a carrier's own base stations. *See, e.g.*, Harris Wireless Products Group, Product Description, 1 ("Active interrogation capability emulates base stations"), http://servv89pn0aj.sn.sourcedns.com/~gbpprorg/2600/Harris_StingRay.pdf. Those signals "penetrate walls" (necessarily, to provide connectivity indoors). *What You Need to Know About Your Network*, AT&T, http://www.att.com/gen/press-room?pid=14003; *see also* E.H. Walker, *Penetration of Radio Signals Into Buildings in the Cellular Radio Environment*, 62 THE BELL SYSTEMS TECHNICAL JOURNAL 2719 (1983), http://www.alcatel-lucent.com/bstj/vol62-1983/articles/bstj62-9-2719.pdf.

cases "within an accuracy of 2 m[eters]."[16] *United States v. Rigmaiden,* a tax fraud prosecution, is one of the few cases in which the government's use of the device has come to light. In it, the government conceded that agents used the device while wandering around an apartment complex on foot, and that the device ultimately located the suspect while he was inside his unit. *See United States v. Rigmaiden*, 2013 WL 1932800, at *15 (D. Ariz. May 8, 2013).[17]

Third, stingrays impact third parties on a significant scale. In particular, they capture information from third parties by mimicking a wireless company's network equipment and thereby triggering an automatic response from all mobile devices on the same network in the vicinity.[18] The government in *Rigmaiden* conceded as much. *See id.* at *20.

Fourth, the devices can be configured to capture the actual content of phone calls or text messages.[19]

Fifth, the government has failed to disclose crucial details about its use of stingray technology – even to the magistrate judges who oversee and approve electronic surveillance applications. In the *Rigmaiden* matter, the government sought court authorization from then-Magistrate Judge Seeborg to use a stingray, but the application did not indicate that the device at issue was a stingray and "did not disclose that the … device would capture signals from other

---

[16] *See, e.g.*, PKI Electronic Intelligence GmbH, *GSM Cellular Monitoring Systems*, 12 (device can "locat[e] ... a target mobile phone within an accuracy of 2 m[eters]"), http://www.docstoc.com/docs/99662489/GSM-CELLULAR-MONITORING-SYSTEMS---PKI-Electronic-#.

[17] Although the criminal prosecution is pending in the District of Arizona, the orders authorizing use of the stingray device were issued in the Northern District of California by then-Magistrate Judge Seeborg. *See Rigmaiden*, 2013 WL 1932800 at *3.

[18] *See, e.g.*, Hannes Federrath, *Protection in Mobile Communications*, MULTILATERAL SECURITY IN COMMUNICATIONS, 5 (Günter Müller et al. eds., 1999) ("possible to determine the IMSIs of all users of a radio cell"), *available at* http://epub.uni-regensburg.de/7382/1/Fede3_99Buch3Mobil.pdf; Daehyun Strobel, *IMSI Catcher*, Seminararbeit, Ruhr-Universität, Bochum, Germany, 13 (July 13, 2007) ("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."), *available at* http://www.emsec.rub.de/media/crypto/attachments/files/2011/04/imsi_catcher.pdf.

[19] *See, e.g.*, Ability, "Active GSM Interceptor: IBIS II - In-Between Interception System - 2nd Generation" ("Real Time Interception for voice and SMS"), *available at* http://www.interceptors.com/intercept-solutions/Active-GSM-Interceptor.html.

cells phones … in the area." *Id.* A May 23, 2011 email obtained from the U.S. Attorney's Office for the Northern District of California through a Freedom of Information Act lawsuit indicates that the *Rigmaiden* application was not unique: The email describes how federal agents *in this judicial district* were using stingray "technology in the field" even though applications submitted to the court did "not make that explicit"; the email further indicates that magistrates in the Northern District of California had expressed "collective concerns" about some aspects of the government's use of this technology. *See* Defs' Exh. O (ECF No. 230) at 1.

b. Stingrays Raise Myriad Fourth Amendment Problems

Stingray technology gives rise to numerous constitutional violations.

First, there is a serious question whether stingray technology – because of its inevitable impact on third parties – can ever be used consistent with the Fourth Amendment. The Fourth Amendment was "the product of [the Framers'] revulsion against" "general warrants" that provided British "customs officials blanket authority to search where they pleased for goods imported in violation of the British tax laws." *Stanford v. Texas*, 379 U.S. 476, 481-82 (1965). Stingrays, however, inevitably scoop up information about innocent third parties as to whom there is no probable cause. *See United States v. Spilotro*, 800 F.2d 959, 963 (9th Cir. 1986) (Fourth Amendment "prevents general, exploratory searches and indiscriminate rummaging through a person's belongings").

Second, and at a minimum, the government's use of these devices constitutes a search within the meaning of the Fourth Amendment. By pinpointing suspects and third parties when they are inside homes and other private locations, stingrays invade reasonable expectations of privacy. *See Kyllo v. United States*, 533 U.S. 27, 34 (2001) (thermal imaging to detect heat from home constituted search); *United States v. Karo*, 468 U.S. 705, 715 (1984) (monitoring of beeper placed into can of ether that was taken into residence constituted search). In addition, stingrays involve a trespass; they send electronic signals to penetrate the walls of everyone living nearby in order to seek information about interior spaces. *See Silverman v. United States*, 365 U.S. 505, 509 (1961) (use of "spike mike," a microphone attached to spike inserted into

walls of house, constituted "unauthorized physical penetration into the premises" giving rise to a search); *Jones*, 132 S. Ct. at 949 (installation and monitoring of GPS on suspect's vehicle constituted search because of "physical intrusion" "for the purpose of obtaining information"). Further, to the extent the government uses stingray devices while walking on foot immediately outside people's homes to ascertain information about interior spaces, it impermissibly intrudes on constitutionally protected areas. *See Florida v. Jardines*, 133 S. Ct. 1409 (2013) (government's entry into curtilage with trained dogs to sniff for drugs inside home constitutes search). As a result, use of a stingray is presumptively invalid unless the government obtains a warrant.

Third, assuming stingray use is not *per se* unconstitutional, and even in those instances where the government obtains a warrant, the warrant materials must be reviewed to ensure that the government provided the magistrate with material information about the technology. Given the heightened risk of intrusive searches posed by advances in technology, "the government's duty of candor in presenting a warrant application," *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1178 (9th Cir. 2010), requires it to explain to magistrates the technology and "the process by which the technology will be used to engage in the electronic surveillance." *See In re Application for an Order Authorizing Installation and Use of a Pen Register and Trap and Trace Device*, 890 F. Supp. 2d 747, 749 (S.D. Tex. 2012) (denying application pursuant to pen register statute to use stingray device where application failed to "explain the technology"). An understanding of "the technology involved" is necessary to "appreciate the constitutional implications of" the warrant application, particularly where, as with stingrays, the technology entails "a very broad and invasive search affecting likely hundreds of individuals in violation of the Fourth Amendment." *In re Application for an Order Pursuant to 18 U.S.C. § 2703(d)* (*In re Cell Tower Dump*), 930 F. Supp. 2d 698, 702 (S.D. Tex. 2012) (denying statutory application for request for cell site records of all subscribers from

several cell towers). A magistrate cannot exercise her constitutional function of supervising the search, unless presented with all material facts. Information about how the technology works is necessary for the magistrate to craft "explicit limitations … to prevent an overly intrusive search." *United States v. Rettig*, 589 F.2d 418, 423 (9th Cir. 1978).[20] Thus, evidence that a search warrant was obtained pursuant to an affidavit that deliberately omitted key information is material to a defendant's suppression motion. *See infra* at Part B-3.

B. *Brady* and Rule 16 Require The Government To Disclose To Defendants The Full Extent Of The Electronic Surveillance Used In This Investigation

The government's obligations under *Brady v. Maryland*, 373 U.S. 83 (1963), and Fed. R. Crim. P. 16 extend to information relevant to a Fourth Amendment motion to suppress. Defendants are therefore entitled to disclosure of the full extent of the electronic surveillance used in this case, in particular, any reliance on NSA-derived call data, the Hemisphere Project, and/or stingrays. Given the unconstitutionality of these intrusive surveillance programs and devices, *see supra* Part II-A, defendants have a right to information showing whether the government relied on them; for if it did, defendants would have more than a reasonable probability of prevailing on a motion to suppress. *See United States v. Gamez-Orduno*, 235 F.3d 453, 461 (9th Cir. 2000) ("[S]uppression of material evidence helpful to the accused, whether at trial or on a motion to suppress, violates due process if there is a reasonable probability that, had the evidence been disclosed, the result of the proceeding would have been different.").

1. The Government Has Failed To Disclose Significant Sources Of Information On Which It Relied To Obtain Wiretaps

The information provided to defendants about the investigation contains obvious and substantial gaps.

---

[20] Such limitations might include judicially developed protocols for how to handle third-party data, *cf., e.g.*, *CDT*, 621 F.3d at 1180 (proposing "[s]egregation and redaction" of third-party information "by specialized personnel or an independent third party") (Kozinski, C.J., concurring), and an express prohibition on capturing content absent compliance with the heightened requirements for a wiretap set forth in 18 U.S.C. §2518.

This case is a multi-defendant prosecution for drug distribution and other drug-related offenses. *See* Defs' Mot. to Compel (ECF No. 226) at 3. The investigation spanned from San Francisco to the Pacific Northwest. *See, e.g.*, Defs' Exh. P (ECF No. 230) ¶ 8.

In the course of this investigation, the government obtained call detail records for 742,907 phone calls. It produced to defendants a spreadsheet with the call data, which consisted of the "target" phone number (or other unique identifying number), number dialed or dialing in, date, time, and duration of the call, and in some cases location information. The spreadsheet revealed that at least 643 different unique identifying numbers are listed as 'target' phones, but the government produced court orders authorizing collection of call data for only 52 numbers. Thus, the government acquired CDRs on *591 numbers* not identified in any of the court orders produced to defendants. *See* Defs' Mot. to Compel (ECF No. 226) at 23-24. This enormous discrepancy between the call data actually collected and the court orders authorizing such collection raises substantial questions about whether the government has failed to produce documents or information identifying the source of much of the call data.

When queried about how the government acquired such voluminous call data, the Assistant United States Attorney suggested that the data had been obtained by "administrative subpoena." *Id.* at 24.

While there are large gaps in what the government has produced to date, the orders that have been disclosed are telling. At various points in the investigation when a target ceased using a particular phone that was being monitored, the government was quickly able to identify the target's new phone – yet it has hardly explained how it accomplished this feat, saying only that it relied on undisclosed "confidential source[s]." *See, e.g.*, Defs' Exh. Q (ECF No. 230) at Bates 01001350 ¶ d (Sprint suspended service on target's phone on August 8, 2009; two days later "a confidential source (previously identified as SOI-1) provided investigating agents with a new cellular telephone number").

It is thus clear that the government has not disclosed all sources of cell phone data. Such sources consist at a minimum of the following two types of information (1) all sources of

information for the approximately 750,000 calls involving at least 643 target numbers and (2) the sources of information that mysteriously and quickly allowed the government to ascertain replacement phones, and for which the government then sought additional court orders authorizing it to obtain additional call data. This is despite the fact that the government relied heavily on the cell phone data in obtaining authorization for the wiretaps. *See* Defs' Mot. to Compel (ECF No. 226) at 20-23.

2. The Government's Disclosures Strongly Suggest Its Investigation Relied On Unconstitutional Surveillance Programs Such As Hemisphere

At the same time, the evidence strongly suggests that the government relied in this investigation on the unconstitutional surveillance programs described above, including Hemisphere.

This case involved the investigation of a drug trafficking ring in California and the Northwest – exactly the geographic and subject-matter focus of the Hemisphere Project, as detailed in the training slides disclosed by the New York Times. *See* Hemisphere Slide Deck at 1-2, 4. The government acquired call detail records for almost three-quarters of a million phone calls. *Cf. id.* at 2 (4 billion CDRs populate Hemisphere each day). It appears to have acquired at least some of these CDRs by administrative subpoena (*see* Defs' Mot. to Compel (ECF No. 226) at 24), the process contemplated by Hemisphere. *See* Hemisphere Slide Deck at 2 ("Hemisphere provides electronic call detail records (CDRs) in response to federal, state, and local administrative/grand jury subpoenas."). [21]

Perhaps most significantly, the government in this investigation was able to quickly

---

[21] To the extent these CDRs contained location information, using an administrative subpoena would be at odds with the government's public position on the appropriate legal process for acquiring cell site location information from a carrier – a court order under 18 U.S.C. §2703(d). *See, e.g.*, *In re Application of U.S. for Historical Cell Site Data*, 724 F.3d 600 (5th Cir. 2013). While *amici* contend that the Fourth Amendment instead requires the government to obtain a probable cause warrant for such data, a Section 2703(d) order is in any event different than a subpoena; the standard for disclosure is greater and it requires judicial action. *See* 18 U.S.C. §2703(d) (which requires "specific and articulable facts" that "the records or other information sought, are relevant and material to an ongoing criminal investigation").

identify replacement phones as the targets of its drug investigation discarded old ones. *See, e.g.*, Defs' Exh. Q (ECF No. 230). That ability is one of Hemisphere's "[u]nique [p]roject [f]eatures." *See* Hemisphere Slide Deck at 5. Indeed, "Hemisphere is most often used by DEA … in the Northwest [High Intensity Drug Trafficking Area] to identify replacement/additional phones." *Id.* at 4; *see also id.* at 5 ("the program" can "find the new number" when target drops a phone; "the program can often determine cell phones the target is using that are unknown to law enforcement"). And, consistent with Hemisphere, here Defendants' new phone numbers were identified because they were being "used by [Defendants] in a similar fashion, with similar calling patterns and similar common callers to [their old phones]." Defs' Mot. to Compel (ECF No. 226) at 21 (quoting Bates 1000051-53).

The fact that the government's affidavits nowhere mention Hemisphere or other surveillance programs is not surprising. "All requestors are instructed to never refer to Hemisphere in any official document." *Id.* at 12. In much the same way, recently disclosed government training materials show that DEA agents who receive tips based on NSA surveillance are instructed to manufacture an alternative basis for their investigation and the resulting evidence, in order to obscure the original source of the information. *See* "U.S. Directs Agents To Cover Up Programs," *supra* note 8 (Document obtained by *Reuters* "specifically directs agents to omit the SOD's involvement [in funneling NSA-derived information] from investigative reports, affidavits, discussions with prosecutors and courtroom testimony. Agents are instructed to then use 'normal investigative techniques to recreate the information provided by SOD.'"). This practice effectively covers up the true source of the government's investigation, ensuring that the defendant never has the opportunity to challenge the legality of controversial tactics, such as the surveillance programs at issue here. *See id.* (describing example where federal agent sought to conceal reliance on NSA intercept).

The ease with which the government in this investigation identified new phone numbers used by its targets would also be consistent with its use of stingrays. *See* "How 'Stingray' Devices Work," *supra* note 14 (by "point[ing] the antenna at a location," stingray can collect

number associated with phone "in a given place at a given time").

3. Information About The Electronic Surveillance Used In This Case Is Material To The Defense

As discussed above, the government obtained information from sources it has not disclosed to the defense, but which it used to obtain wiretaps. *See supra* Part II-B-1. This Court should order disclosure of information pertaining to these sources, whether they belong to Hemisphere or any other surveillance program or device not previously disclosed. Information about the sources of the extensive cell phone data acquired and relied upon by the government in this case is material to the defense, in particular, a motion to suppress.

The Fifth Amendment's guarantee of due process requires the government to disclose to the defense any evidence "favorable to an accused" and "material either to guilt or to punishment." *Brady*, 373 U.S. at 87. Evidence is "material" if "there is a reasonable probability that its disclosure would have affected the outcome of the proceedings." *United States v. Guzman-Padilla*, 573 F.3d 865, 890 (9th Cir. 2009) (internal quotation marks, citation omitted). Federal Rule of Criminal Procedure 16 helps effectuate these constitutional rights by granting "criminal defendants a broad right to discovery," including the requirement that the government disclose "documents" or "data" in "the government's possession, custody, or control" that are "material to preparing the defense." *United States v. Stever*, 603 F.3d 747, 752 (9th Cir. 2010) (quoting Fed. R. Crim. P. 16(a)(1)(E)(i)). *Brady*'s discovery obligations extend to facts relevant to raising Fourth Amendment challenges. *See Gamez-Orduno*, 235 F.3d at 461 ("The suppression of material evidence helpful to the accused, whether at trial or on a motion to suppress, violates due process").

The information sought by defendants is material for three reasons.

First, information that sheds light on whether the government relied on NSA-derived data, Hemisphere, or stingrays is material to a motion to suppress because it would allow defendants to challenge the constitutionality of any intrusive surveillance programs to which

they were subjected. There are significant gaps in the sources of the cell phone information obtained by the government, gaps that are likely explained by the government's reliance on Hemisphere or other forms of electronic surveillance. *See supra* at Part II-B-1&2. These intrusive surveillance programs and devices are unconstitutional. *See supra* at Part II-A. "Rule 16 permits discovery that is 'relevant to the development of a possible defense.'" *United States v. Mandel*, 914 F.2d 1215, 1219 (9th Cir. 1990). Defendants should therefore be permitted to develop through discovery information about the extent of the government's reliance on unconstitutional electronic surveillance in this investigation.

Second, *Brady* requires the disclosure of evidence that "bears on the credibility of a significant witness in the case." *United States v. Strifler*, 851 F. 2d 1197, 1201 (9th Cir. 1988); *see also Giglio v. United States*, 405 U.S. 150, 154 (1972). This requirement applies even if the "witness" is electronic surveillance.

Disclosure obligations apply to information about the reliability of "witnesses" the government does not call at trial and that are not human. For example, the government must disclose records about a drug detecting dog, including training and certification records and the "handler's log," in order to allow the defense to assess the dog's reliability and effectively cross-examine the handler at a suppression hearing. *United States v. Thomas*, 726 F.3d 1086, 1096 (9th Cir. 2013) (citing *United States v. Cedano–Arellano*, 332 F.3d 568, 570-71 (9th Cir. 2003)); *see also United States v. Cortez–Rocha*, 394 F.3d 1115, 1118 n.1 (9th Cir. 2005) (disclosure of drug detecting dog evidence is "mandatory"). The Supreme Court explained earlier this year that a criminal defendant must be able to challenge the reliability of a drug detecting dog, noting specifically that the dog's performance in the field may be relevant. *Florida v. Harris*, 133 S. Ct. 1050, 1057 (2013). "[C]ircumstances surrounding a particular alert may undermine the case for probable cause" in some instances. *Id.* at 1057-58.

Brady and Rule 16 disclosure requirements apply equally to dogs and the covert use of surveillance programs. A drug detecting dog's performance is relevant to assessing the dog's credibility for purposes of a suppression motion. To the extent Hemisphere or other

surveillance programs served as the "confidential source … provid[ing] investigating agents with … new cellular telephone number[s]" of the targets of the investigation, Defs' Exh. Q (ECF No. 230) at Bates 01001350, so too is information about how these programs function. And just as the "circumstances surrounding a particular alert" may undermine probable cause in a dog sniff situation, *Harris*, 133 S. Ct. at 1057, the same is true of information about the "algorithm and advanced search features" used by Hemisphere "to find the new number." *See* Hemisphere Slide Deck at 5. Indeed, the government acknowledges that the replacement phone numbers identified by Hemisphere are only "ranked by probability." *Id.* at 7. Under *Brady* and Rule 16, the defense is entitled to information that would allow cross-examination over the reliability of these surveillance programs.

Third, due process prohibits the government's deliberate omission of information necessary to bring a suppression motion. In *United States v. Barton*, 995 F.2d 931, 934 (9th Cir. 1993), the Ninth Circuit held that the deliberate destruction of evidence that would allow a defendant to impeach the officer who submitted a search warrant affidavit violates "the due process principles announced in *Brady*." *Id.* at 935. *Barton* relied on *Franks v. Delaware,* 438 U.S. 154 (1978), which held that defendants have a right to challenge deliberately falsified statements submitted in support of a search warrant application. *Barton,* 995 F.2d at 934-35. The underlying rationale of both *Barton* and *Franks* is that "an officer" should not be permitted to "feel secure that false allegations in his or her affidavit for a search warrant could not be challenged." *Barton*, 995 F.3d at 935; *see also Franks,* 438 U.S. at 168 (Fourth Amendment's probable cause requirement "would be reduced to a nullity if a police officer was able to use deliberately falsified allegations to demonstrate probable cause, and, having misled the magistrate, then was able to remain confident that the ploy was worthwhile").

This same rationale prohibits the deliberate *omission* of information necessary for a successful motion to suppress. *Cf. United States v. Stanert*, 762 F.2d 775, 780-81 (9th Cir. 1985) ("[W]e expressly hold that the Fourth Amendment mandates that a defendant be permitted to challenge a warrant affidavit valid on its face when it contains deliberate or

reckless omissions of facts that tend to mislead."). Here, publicly available evidence suggests that law enforcement agents are intentionally omitting relevant information about their investigations, even in "official document[s]." Hemisphere Slide Deck at 12 ("never refer to Hemisphere"); *see also* "U.S. Directs Agents To Cover Up Programs," *supra* note 8 (agents directed to omit reference to NSA-derived information and instead "recreate" information provided). An internal email from the U.S. Attorney's Office *in this district* indicates that federal agents were using stingray technology "without making that explicit" in pen register applications to this Court. *See* Defs' Exh. O (ECF No. 230) at 1. Due Process should prohibit, and not reward, such intentional omissions, as they would allow the government to "feel secure" that its reliance on unlawful forms of electronic surveillance "could not be challenged." *Barton*, 995 F.2d at 935.

In sum, *Brady* and Rule 16 require disclosure of all of the sources of the cell phone data obtained by the government in this investigation. This includes the sources of the 750,000 calls identified on the spreadsheet produced to defendants and the "confidential sources" that supplied new phone numbers. The Fourth Amendment right to be free from unconstitutional electronic surveillance "would be reduced to a nullity" (*Franks,* 438 U.S. at 168) if the government were permitted to conceal from Defendants and the Court factual information about the extent to which the government relied on Hemisphere or other unconstitutional forms of electronic surveillance to further the investigation.

C. By Shrouding Its Surveillance Practices In Secrecy, The Government Prevents Courts from Reviewing Its Practices

Information about the intrusive and powerful surveillance techniques used to investigate Defendants is clearly essential to this criminal proceeding. But it also has a significance far beyond this case. Disclosure of the information sought is necessary to prevent the government from immunizing controversial surveillance practices from judicial and public scrutiny.

"It may very well be that, given full disclosure of" the government's surveillance practices, "the people and their elected representatives would heartily approve without a second

thought. But then again, they might not." *In re Sealing and Non-Disclosure of Pen/Trap/2703(d) Orders*, 562 F. Supp. 2d 876, 886 (S.D. Tex. 2008) ("*In re Sealing*").[22]

While access to this information is fundamental to our open system of government in general, it is particularly important where the government seeks to use new technology to engage in surveillance. This is so because new forms of technology often raise novel constitutional questions. *See supra* at Part A.

But the government goes to great lengths to keep its surveillance practices secret not only from the public, but even from the courts. It takes affirmative measures to obscure its reliance in criminal investigations on controversial surveillance sources, like Hemisphere or NSA-derived intelligence, in documents presented to the Court. *See* Hemisphere Slide Deck at 12 (agents "instructed to never refer to Hemisphere in any official document"); "U.S. Directs Agents To Cover Up Programs," *supra* note 8 (Document obtained by *Reuters* directs agents to omit reference to NSA-derived information from affidavits and courtroom testimony and to use "'normal investigative techniques to recreate the information provided'"). Agents in this district have apparently used stingray technology "without making that explicit" in accompanying applications to this Court. *See* Defs' Exh. O (ECF No. 230) at 1. Even in those instances when the government sets forth its surveillance practices in applications for court orders, the public has few methods for accessing this information.[23]

---

[22] Judge Smith has identified a troubling phenomenon of permanently sealed electronic surveillance dockets in district courts around country. Government applications for electronic surveillance are typically filed under seal "until further order of the Court"; but because the government rarely moves to unseal these orders, they typically remain sealed indefinitely. *See id.* at 877-78; *see also* Stephen Wm. Smith, *Gagged, Sealed & Delivered: Reforming ECP's Secret Docket*, 6 Harv. L. & Pol'y Rev. 313, 322 (2012) (estimating that federal magistrate judges issued more than 30,000 orders for electronic surveillance under seal in 2006, "more than thirty times the annual number of [Foreign Intelligence Surveillance Act] cases"). Based on the First Amendment and common law right of access to judicial records, Judge Smith therefore announced that he would follow a new protocol, sealing electronic surveillance orders only for six months, after which sealing orders would automatically expire absent a showing of need by the government for continued sealing. *Id.* at 895.

[23] The Department of Justice is at present vigorously opposing Freedom of Information Act litigation seeking applications for electronic surveillance involving location tracking and filed

By keeping this information secret, the government, whether intentionally or not, immunizes itself from popular, legislative, and legal challenges to its surveillance practices. Because the government seeks court authorization – either statutory orders or probable cause warrants – to engage in location tracking in *ex parte* proceedings, magistrates reviewing such applications lack the benefit of the adversarial process in deciding these complex legal issues. This has the potential to create serious distortions in the development of surveillance law, by allowing the executive branch excessive authority in "making" the law.

Perhaps it is not surprising that the government actively resists disclosure of information about its surveillance practices in Freedom of Information Act cases. But if the government is able to hide this information even from criminal defendants who have been subjected to intrusive surveillance, then these practices will escape all court review and the executive will effectively be allowed to make surveillance law unilaterally and secretly. Our constitutional system does not tolerate such a result.

//

//

//

//

//

//

---

by the United States' Attorneys Office for the Northern District of California in this Court. DOJ has asserted that it should not even have to search for records (let alone produce them) because most of the records are under seal and it has *no* process for systematically ascertaining "whether the conditions requiring sealing continue." *See ACLU of Northern California v. Dep't of Justice*, N.D. Cal. Case No. 12-cv-04008-MEJ, ECF Nos. 43 at 18; 43-1 ¶ 9 (excerpts attached as Lye Decl., Exhs. 2 & 3. The government is thus keeping its surveillance practices secret, long after the actual need for secrecy dissolves. Judge Smith's observation about the Southern District of Texas is thus equally apt in this judicial district: "indefinitely sealed means permanently sealed." *In re Sealing*, 562 F. Supp. 2d at 878.

III. CONCLUSION

For the foregoing reasons, the Court should grant Defendants' motion to compel.

Dated: October 15, 2013

Respectfully Submitted,

By: /s/ *Linda Lye*
Linda Lye

Linda Lye
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF NORTHERN CALIFORNIA
39 Drumm Street, 2nd Floor
San Francisco, California 94111
Telephone: 415-621-2493
Facsimile: 415-255-8437

Attorneys for *Amicus* American Civil Liberties Union of Northern California

Ezekiel Edwards (eedwards@aclu.org)
Nathan Freed Wessler (nwessler@aclu.org)
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Telephone: 212-549-2500
Facsimile: 212-549-2654

Attorneys for *Amicus* American Civil Liberties Union

Hanni M. Fakhoury
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: 415-436-9333
Facsimile: 415-436-9993

Attorneys for *Amicus* Electronic Frontier Foundation