

1 Linda Lye (CA SBN 215584)
lye@aclunc.org
2 AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF NORTHERN CALIFORNIA
3 39 Drumm Street, 2nd Floor
San Francisco, California 94111
4 Telephone: 415-621-2493
5 Facsimile: 415-255-8437

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

7 Ezekiel Edwards (eedwards@aclu.org)
8 Nathan Freed Wessler (nwessler@aclu.org)
AMERICAN CIVIL LIBERTIES UNION
9 FOUNDATION
10 125 Broad Street, 18th Floor
New York, NY 10004
11 Telephone: 212-549-2500
Facsimile: 212-549-2654

12 ATTORNEYS FOR *AMICUS*
13 AMERICAN CIVIL LIBERTIES UNION

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

18 ATTORNEYS FOR *AMICUS*
19 ELECTRONIC FRONTIER FOUNDATION

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

22 UNITED STATES OF AMERICA,

23 Plaintiff,

24 v.

25 DIAZ-RIVERA, et al.,

26 Defendants.
27
28

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

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

- I. INTRODUCTION 1
- II. ARGUMENT 1
 - A. The NSA Mass Call-Tracking Program, The Hemisphere Project, And Stingray Devices Are Unconstitutional 1
 - 1. The National Security Agency’s Mass Call-Tracking Program..... 1
 - a. The Federal Government Has Amassed A Vast Database Of Americans’ Call Records 1
 - b. The Warrantless Bulk Collection Of Phone Records Is Unconstitutional..... 3
 - 2. The Hemisphere Project..... 5
 - a. The Federal Government Has Amassed Yet Another Vast Database Of Americans’ Call Records 5
 - b. The Government Cannot Launder Its Unconstitutional Bulk Collection Of Phone Records Through AT&T..... 6
 - 3. Stingrays 8
 - a. Stingrays Scoop Up Information From Innocent Third Party Wireless Devices 8
 - b. Stingrays Raise Myriad Fourth Amendment Problems 10
 - B. *Brady* and Rule 16 Require The Government To Disclose The Full Extent Of The Electronic Surveillance Used In This Investigation..... 12
 - 1. The Government Has Failed To Disclose Significant Sources Of Information On Which It Relied To Obtain Wiretaps 12
 - 2. This Investigation Is Consistent With Unconstitutional Surveillance Programs Such As Hemisphere 14
 - 3. Information About The Electronic Surveillance Used In This Case Is Material To The Defense 16

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

C. By Shrouding Its Surveillance Practices In Secrecy, The
Government Stifles Public Debate And Prevents Courts
from Reviewing Its Practices 19

III. CONCLUSION..... 22

TABLE OF AUTHORITIES

Cases

Page(s)

Brady v. Maryland,
373 U.S. 83 (1963).....12, 16, 17, 18

Florida v. Harris,
133 S. Ct. 1050 (2013).....17

Florida v. Jardines,
133 S. Ct. 1409 (2013).....11

Franks v. Delaware,
438 U.S. 154 (1978).....18

Giglio v. United States,
405 U.S. 150 (1972).....17

*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).....11

In re Application for an Order Pursuant to 18 U.S.C. § 2703(d),
930 F. Supp. 2d 698 (S.D. Tex. 2012)11

*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)2

In re Application of U.S. for Historical Cell Site Data,
724 F.3d 600 (5th Cir. 2013)14

In re Sealing and Non-Disclosure of Pen/Trap/2703(d) Orders,
562 F. Supp. 2d 876 (S.D. Tex. 2008)20

Jewel v. Nat’l Sec. Agency,
673 F.3d 902 (9th Cir. 2011)7

Kyllo v. United States,
533 U.S. 27 (2001).....10

NAACP v. Alabama ex rel. Patterson,
357 U.S. 449 (1958).....4

Silverman v. United States,
365 U.S. 505 (1961).....10

1 *Stanford v. Texas*,
2 379 U.S. 476 (1965).....10

3 *United States v. Barton*,
4 995 F.2d 931 (9th Cir. 1993)18

5 *United States v. Comprehensive Drug Testing, Inc.*,
6 621 F.3d 1162 (9th Cir. 2010)11, 12

7 *United States v. Cortez-Rocha*,
8 394 F.3d 1115 (9th Cir. 2005)17

9 *United States v. Gamez-Orduno*,
10 235 F.3d 453 (9th Cir. 2000)12, 16

11 *United States v. Guzman-Padilla*,
12 573 F.3d 865 (9th Cir. 2009)16

13 *United States v. Jones*,
14 132 S. Ct. 945 (2012).....4, 7, 11

15 *United States v. Karo*,
16 468 U.S. 705 (1984).....10

17 *United States v. Mandel*,
18 914 F.2d 1215 (9th Cir. 1990) 17

19 *United States v. Reed*,
20 15 F.3d 928 (9th Cir. 1994)7

21 *United States v. Rettig*,
22 589 F.2d 418 (9th Cir. 1978)12

23 *United States v. Rigmaiden*,
24 2013 WL 1932800 (D. Ariz. May 8, 2013)9, 10

25 *United States v. Ruby*,
26 2013 WL 544888 (S.D. Cal. Feb. 12, 2013).....6

27 *United States v. Spilotro*,
28 800 F.2d 959 (9th Cir. 1986)10

United States v. Stanert,
762 F.2d 775 (9th Cir. 1985)18

United States v. Stever,
603 F.3d 747 (9th Cir. 2010)16

1 *United States v. Strifler*,
2 851 F. 2d 1197 (9th Cir. 1988)17

3 *United States v. Thomas*,
4 726 F.3d 1086 (9th Cir. 2013)17

5 **Statutes**

6 18 U.S.C. § 2518.....12

7 18 U.S.C. § 2703.....6, 14

8 **Rules**

9 Fed. R. Crim. P. 16 *passim*

10 **Congressional Materials**

11 Oversight of FISA (Foreign Intelligence Surveillance Act) Surveillance Programs:
12 Hearing of the Senate Judiciary Committee on Strengthening Privacy Rights and
13 National Security, 113th Cong. (2013) (oral testimony of Sean Joyce)2

14 **Other Authorities**

15 Ability, “Active GSM Interceptor: IBIS II - In-Between Interception System - 2nd
16 Generation,”9

17 ADMINISTRATION WHITE PAPER: BULK COLLECTION OF TELEPHONY METADATA UNDER
18 SECTION 215 OF THE USA PATRIOT ACT 1 (Aug. 9, 2013)2

19 Federal Bureau of Investigation, Press Release, San Diego Division, San Diego Jury Convicts
20 Four Somali Immigrants of Providing Support to Foreign Terrorists
21 (Feb. 22, 2013)3

22 Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers*
23 *Daily*, THE GUARDIAN (June 5, 2013).....2

24 Hannes Federrath, *Protection in Mobile Communications*, MULTILATERAL SECURITY IN
25 COMMUNICATIONS, 5 (Günter Müller et al. eds., 1999).....9

26 Harris Wireless Products Group, Product Description, 18

27 Office of the Director of National Intelligence, DNI Statement on Recent
28 Unauthorized Disclosures of Classified Information (June 6, 2013).....2

Office of the Director of National Intelligence, Press Release, Foreign Intelligence
Surveillance Court Renews Authority to Collect Telephony Metadata (July 19, 2013)2

1 PKI Electronic Intelligence GmbH, *GSM Cellular Monitoring Systems*, 129

2 Scott Shane & Colin Moynihan, *Drug Agents Use Vast Phone Trove, Eclipsing N.S.A. 's*, N.Y.

3 TIMES (Sept. 1, 2013).....5

4 John Shiffman & Kristina Cooke, *U.S. Directs Agents To Cover Up Programs*

5 *Used To Investigate Americans*, REUTERS (Aug. 5, 2013)3, 15, 18, 20

6 Stephen Wm. Smith, *Gagged, Sealed & Delivered: Reforming ECP's Secret Docket*,

7 6 Harv. L. & Pol'y Rev. 313, 322 (2012)20

8 Daehyun Strobel, *IMSI Catcher*, Seminararbeit, Ruhr-Universität, Bochum, Germany, 13

9 (July 13, 2007)9

10 *Synopsis of the Hemisphere Project*, N.Y. TIMES (Sept. 1, 2013)5

11 Jennifer Valentino-DeVries, *How 'Stingray' Devices Work*, WALL STREET JOURNAL

12 (Sept. 21, 2011).....8

13 E.H. Walker, *Penetration of Radio Signals Into Buildings in the Cellular Radio*

14 *Environment*, 62 THE BELL SYSTEMS TECHNICAL JOURNAL 2719 (1983)8

15

16

17

18

19

20

21

22

23

24

25

26

27

28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18

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

19
20

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

21

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

22

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

23
24
25
26
27
28

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

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

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

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

15
16 ¹ *In re Application of the FBI for an Order Requiring the Production of Tangible Things from*
17 *Verizon Bus. Network Servs., Inc. on Behalf of MCI Commc'n Servs., Inc. d/b/a Verizon Bus.*
18 *Servs.*, No. BR 13-80 at 2 (FISA Ct. Apr. 25, 2013), available at
19 <http://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order>;
20 see also Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers*
21 *Daily*, THE GUARDIAN (June 5, 2013), available at
22 <http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>. In the
23 days after *The Guardian* disclosed the Secondary Order, Director of National Intelligence James
24 Clapper acknowledged its authenticity. See Press Release, Office of the Director of National
25 Intelligence, DNI Statement on Recent Unauthorized Disclosures of Classified Information
26 (June 6, 2013), available at <http://1.usa.gov/13jwuFc>.

27 ² Press Release, Office of the Director of National Intelligence, Foreign Intelligence
28 Surveillance Court Renews Authority to Collect Telephony Metadata (July 19, 2013), available
at <http://1.usa.gov/12ThYIT>.

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 at 10-11, 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

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

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

16 **b. The Warrantless Bulk Collection Of Phone Records Is Unconstitutional**

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

19
20
21 instance when we used the business record 215 program, as Chairman Leahy mentioned,
22 Basaaly Moalin.”).

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

26 ⁷ *ACLU v. Clapper*, S.D.N.Y. Case No. 13-cv-03994, Defs’ Mem. of Law in Opposition to Pls.’
27 Motion for a Preliminary Injunction at 10-11, ECF No. 61 (Oct. 1, 2013) (“NSA received [a
28 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.*

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

17
18 The mass call-tracking program also violates the First Amendment. The Supreme Court
19 has recognized that the government’s surveillance and investigatory activities can infringe on
20 associational rights protected by the First Amendment. Thus in *NAACP v. Alabama ex rel.*
21 *Patterson*, 357 U.S. 449 (1958), a case in which the Supreme Court invalidated an Alabama
22 order that would have required the NAACP to disclose its membership lists, the Court wrote,
23 “[i]t is hardly a novel perception that compelled disclosure of affiliation with groups engaged in
24 advocacy” may operate as “a restraint on freedom of association.” *Id.* at 462. The
25 government’s mass call-tracking program raises precisely the same specter of associational
26 harm by permitting the government to track every one of Defendants’ telephone contacts.

27 //

28 //

1 **2. The Hemisphere Project**

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

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

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

21 “Hemisphere is most often used by DEA and DHS in the Northwest [High Intensity
22 Drug Trafficking Area] to identify replacement/additional phones.” *Id.* at 4. The project is
23

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

27 ¹² The training slides were posted by the New York Times on its website. *See* Office of Nat’l
28 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>.

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

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

17 **b. The Hemisphere Project Is Unconstitutional**

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

20 The Hemisphere Project is unlike typical government requests to phone companies for
21 CDRs. In run-of-the-mill investigations, the government seeks a judicial order to the phone
22 company and then awaits the results of the company’s compliance. *See, e.g., United States v.*
23 *Ruby*, 2013 WL 544888, at *3 (S.D. Cal. Feb. 12, 2013) (government acquired call detail
24 records from service provider after obtaining and serving order pursuant to 18 U.S.C. §
25 2703(d)). Here, however, the government funds and directs the entire process by paying AT&T
26 to embed its employees within DEA operational units, directing their search of the Hemisphere
27 system, and then obtaining CDRs in a format requested by the DEA. This constitutes state
28 action, as the government has created an agency relationship with embedded AT&T employees

1 and has directed their searches of trillions of call records without warrants. *See United States v.*
2 *Reed*, 15 F.3d 928, 931 (9th Cir. 1994) (“[T]he Fourth Amendment does prohibit unreasonable
3 intrusions by private individuals who are acting as government instruments or agents.”).
4 Hemisphere is functionally indistinguishable from mass surveillance programs where the
5 government installs agents and monitoring equipment in phone company facilities and searches
6 incoming or transiting phone traffic. *Cf. Jewel v. Nat’l Sec. Agency*, 673 F.3d 902, 906 (9th Cir.
7 2011) (holding that plaintiffs have standing to bring Fourth Amendment challenge to NSA
8 surveillance program that diverted all internet traffic passing through AT&T facilities into a
9 “SG3 Secure Room” in those facilities, where “information of interest [was] transmitted from
10 the equipment in the SG3 Secure Rooms to the NSA based on rules programmed by the NSA”
11 (alteration in original) (internal quotation marks omitted)).

12
13 At a minimum, Hemisphere raises similar constitutional concerns as the NSA mass call-
14 tracking database. The government is querying the stored call records of millions of people in
15 the United States in order to identify patterns in the communications and associations of a few
16 individuals. But the program sweeps up the records of millions of individuals who are not the
17 subject of any investigation, amassing their call records even though there is no suspicion they
18 have engaged in criminal wrongdoing, and analyzing their records without a warrant, and hence,
19 without any judicial oversight. This violates the Fourth and First Amendments. *Supra* Part II-
20 A-1-b. But Hemisphere goes even further than the NSA’s mass call-tracking program, as the
21 CDRs stored in the Hemisphere database contain location information about callers (*see*
22 Hemisphere Slide Deck at 3, 13), thus implicating the specific concerns raised by five Justices
23 in *Jones*. *See* 132 S. Ct. at 955 (Sotomayor, J., concurring) (“wealth of detail about [a person’s]
24 familial, political, professional, religious, and sexual associations” revealed through “trips to the
25 psychiatrist, the plastic surgeon, the abortion clinic,” etc.) (internal quotation marks, citation
26 omitted); *id.* at 964 (Alito, J., concurring).

27
28 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

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

4 3. Stingrays

5 a. Stingrays Scoop Up Information From Innocent Third Party 6 Wireless Devices

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

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

19 Second, the devices can pinpoint an individual with extraordinary precision, in some
20

21
22 ¹³ Although “Stingray” refers to a specific line of Harris Corporation products, *see infra* at note
23 15, *amici* use the term “stingray” in this brief generically to refer to IMSI catchers.

24 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/>.

25 ¹⁵ The devices send signals like those emitted by a carrier’s own base stations. *See, e.g.*, Harris
26 Wireless Products Group, Product Description, 1 (“Active interrogation capability emulates
27 base stations”), http://servv89pn0aj.sn.sourcedns.com/~gbpprorg/2600/Harris_StingRay.pdf.
28 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](http://www.alcatel-lucent.com/bstj/vol62-1983/articles/bstj62-9-2719.pdf).

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

6
7 Third, stingrays impact third parties on a significant scale. In particular, they capture
8 information from third parties by mimicking a wireless company’s network equipment and
9 thereby triggering an automatic response from all mobile devices on the same network in the
10 vicinity.¹⁸ The government in *Rigmaiden* conceded as much. *See id.* at *20.

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

13 Fifth, the government has failed to disclose crucial details about its use of stingray
14 technology – even to the magistrate judges who oversee and approve electronic surveillance
15 applications. In the *Rigmaiden* matter, the government sought court authorization from then-
16 Magistrate Judge Seeborg to use a stingray, but the application did not indicate that the device
17 at issue was a stingray and “did not disclose that the ... device would capture signals from other
18

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

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

25 ¹⁸ *See, e.g.*, Hannes Federrath, *Protection in Mobile Communications*, MULTILATERAL
26 SECURITY IN COMMUNICATIONS, 5 (Günter Müller et al. eds., 1999) (“possible to determine the
27 IMSIs of all users of a radio cell”), available at http://epub.uni-regensburg.de/7382/1/Fede3_99Buch3Mobil.pdf; Daehyun Strobel, *IMSI Catcher*,
28 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>.

1 cells phones ... in the area.” *Id.* A May 23, 2011 email obtained from the U.S. Attorney’s
2 Office for the Northern District of California through a Freedom of Information Act lawsuit
3 indicates that the *Rigmaiden* application was not unique: The email describes how federal
4 agents *in this judicial district* were using stingray “technology in the field” even though
5 applications submitted to the court did “not make that explicit”; the email further indicates that
6 magistrates in the Northern District of California had expressed “collective concerns” about
7 some aspects of the government’s use of this technology. *See* Defs’ Exh. O (ECF No. 230) at 1.
8

9 **b. Stingrays Raise Myriad Fourth Amendment Problems**

10 Stingray technology gives rise to numerous constitutional violations.

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

20 Second, and at a minimum, the government’s use of these devices constitutes a search
21 within the meaning of the Fourth Amendment. By pinpointing suspects and third parties when
22 they are inside homes and other private locations, stingrays invade reasonable expectations of
23 privacy. *See Kyllo v. United States*, 533 U.S. 27, 34 (2001) (thermal imaging to detect heat
24 from home constituted search); *United States v. Karo*, 468 U.S. 705, 715 (1984) (monitoring of
25 beeper placed into can of ether that was taken into residence constituted search). In addition,
26 stingrays involve a trespass; they send electronic signals to penetrate the walls of everyone
27 living nearby in order to seek information about interior spaces. *See Silverman v. United States*,
28 365 U.S. 505, 509 (1961) (use of “spike mike,” a microphone attached to spike inserted into

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

10 Third, assuming stingray use is not *per se* unconstitutional, and even in those instances
11 where the government obtains a warrant, the warrant materials must be reviewed to ensure that
12 the government provided the magistrate with material information about the technology. Given
13 the heightened risk of intrusive searches posed by advances in technology, “the government’s
14 duty of candor in presenting a warrant application,” *United States v. Comprehensive Drug*
15 *Testing, Inc.*, 621 F.3d 1162, 1178 (9th Cir. 2010), requires it to explain to magistrates the
16 technology and “the process by which the technology will be used to engage in the electronic
17 surveillance.” *See In re Application for an Order Authorizing Installation and Use of a Pen*
18 *Register and Trap and Trace Device*, 890 F. Supp. 2d 747, 749 (S.D. Tex. 2012) (denying
19 application pursuant to pen register statute to use stingray device where application failed to
20 “explain the technology”). An understanding of “the technology involved” is necessary to
21 “appreciate the constitutional implications of” the warrant application, particularly where, as
22 with stingrays, the technology entails “a very broad and invasive search affecting likely
23 hundreds of individuals in violation of the Fourth Amendment.” *In re Application for an Order*
24 *Pursuant to 18 U.S.C. § 2703(d) (In re Cell Tower Dump)*, 930 F. Supp. 2d 698, 702 (S.D. Tex.
25 2012) (denying statutory application for request for cell site records of all subscribers from
26
27
28

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

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

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

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

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

26 ²⁰ Such limitations might include judicially developed protocols for how to handle third-party
27 data, *cf., e.g., CDT*, 621 F.3d at 1180 (proposing “[s]egregation and redaction” of third-party
28 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.

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

4 In the course of this investigation, the government obtained call detail records for
5 742,907 phone calls. It produced to defendants a spreadsheet with the call data, which consisted
6 of the “target” phone number (or other unique identifying number), number dialed or dialing in,
7 date, time, and duration of the call, and in some cases location information. The spreadsheet
8 revealed that at least 643 different unique identifying numbers are listed as ‘target’ phones, but
9 the government produced court orders authorizing collection of call data for only 52 numbers.
10 Thus, the government acquired CDRs on *591 numbers* not identified in any of the court orders
11 produced to defendants. *See* Defs’ Mot. to Compel (ECF No. 226) at 23-24. This enormous
12 discrepancy between the call data actually collected and the court orders authorizing such
13 collection raises substantial questions about whether the government has failed to produce
14 documents or information identifying the source of much of the call data.

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

18 While there are large gaps in what the government has produced to date, the orders that
19 have been disclosed are telling. At various points in the investigation when a target ceased
20 using a particular phone that was being monitored, the government was quickly able to identify
21 the target’s new phone – yet it has hardly explained how it accomplished this feat, saying only
22 that it relied on undisclosed “confidential source[s].” *See, e.g.*, Defs’ Exh. Q (ECF No. 230) at
23 Bates 01001350 ¶ d (Sprint suspended service on target’s phone on August 8, 2009; two days
24 later “a confidential source (previously identified as SOI-1) provided investigating agents with a
25 new cellular telephone number”).
26

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

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

7 **2. The Government’s Disclosures Strongly Suggest Its Investigation**
8 **Relied On Unconstitutional Surveillance Programs Such As**
9 **Hemisphere**

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

13 This case involved the investigation of a drug trafficking ring in California and the
14 Northwest – exactly the geographic and subject-matter focus of the Hemisphere Project, as
15 detailed in the training slides disclosed by the New York Times. *See* Hemisphere Slide Deck at
16 1-2, 4. The government acquired call detail records for almost three-quarters of a million phone
17 calls. *Cf. id.* at 2 (4 billion CDRs populate Hemisphere each day). It appears to have acquired
18 at least some of these CDRs by administrative subpoena (*see* Defs’ Mot. to Compel (ECF No.
19 226) at 24), the process contemplated by Hemisphere. *See* Hemisphere Slide Deck at 2
20 (“Hemisphere provides electronic call detail records (CDRs) in response to federal, state, and
21 local administrative/grand jury subpoenas.”).²¹

22 Perhaps most significantly, the government in this investigation was able to quickly
23

24 ²¹ To the extent these CDRs contained location information, using an administrative subpoena
25 would be at odds with the government’s public position on the appropriate legal process for
26 acquiring cell site location information from a carrier – a court order under 18 U.S.C. §2703(d).
27 *See, e.g., In re Application of U.S. for Historical Cell Site Data*, 724 F.3d 600 (5th Cir. 2013).
28 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”).

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

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

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

1 number associated with phone “in a given place at a given time”).

2
3 **3. Information About The Electronic Surveillance Used In This Case Is**
4 **Material To The Defense**

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

11 The Fifth Amendment’s guarantee of due process requires the government to disclose to
12 the defense any evidence “favorable to an accused” and “material either to guilt or to
13 punishment.” *Brady*, 373 U.S. at 87. Evidence is “material” if “there is a reasonable
14 probability that its disclosure would have affected the outcome of the proceedings.” *United*
15 *States v. Guzman-Padilla*, 573 F.3d 865, 890 (9th Cir. 2009) (internal quotation marks, citation
16 omitted). Federal Rule of Criminal Procedure 16 helps effectuate these constitutional rights by
17 granting “criminal defendants a broad right to discovery,” including the requirement that the
18 government disclose “documents” or “data” in “the government’s possession, custody, or
19 control” that are “material to preparing the defense.” *United States v. Stever*, 603 F.3d 747, 752
20 (9th Cir. 2010) (quoting Fed. R. Crim. P. 16(a)(1)(E)(i)). *Brady*’s discovery obligations extend
21 to facts relevant to raising Fourth Amendment challenges. *See Gamez-Orduno*, 235 F.3d at 461
22 (“The suppression of material evidence helpful to the accused, whether at trial or on a motion to
23 suppress, violates due process”).

24 The information sought by defendants is material for three reasons.

25 First, information that sheds light on whether the government relied on NSA-derived
26 data, Hemisphere, or stingrays is material to a motion to suppress because it would allow
27 defendants to challenge the constitutionality of any intrusive surveillance programs to which
28

1 they were subjected. There are significant gaps in the sources of the cell phone information
2 obtained by the government, gaps that are likely explained by the government’s reliance on
3 Hemisphere or other forms of electronic surveillance. *See supra* at Part II-B-1&2. These
4 intrusive surveillance programs and devices are unconstitutional. *See supra* at Part II-A. “Rule
5 16 permits discovery that is ‘relevant to the development of a possible defense.’” *United States*
6 *v. Mandel*, 914 F.2d 1215, 1219 (9th Cir. 1990). Defendants should therefore be permitted to
7 develop through discovery information about the extent of the government’s reliance on
8 unconstitutional electronic surveillance in this investigation.
9

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

14 Disclosure obligations apply to information about the reliability of “witnesses” the
15 government does not call at trial and that are not human. For example, the government must
16 disclose records about a drug detecting dog, including training and certification records and the
17 “handler’s log,” in order to allow the defense to assess the dog’s reliability and effectively
18 cross-examine the handler at a suppression hearing. *United States v. Thomas*, 726 F.3d 1086,
19 1096 (9th Cir. 2013) (citing *United States v. Cedano–Arellano*, 332 F.3d 568, 570-71 (9th Cir.
20 2003)); *see also United States v. Cortez–Rocha*, 394 F.3d 1115, 1118 n.1 (9th Cir. 2005)
21 (disclosure of drug detecting dog evidence is “mandatory”). The Supreme Court explained
22 earlier this year that a criminal defendant must be able to challenge the reliability of a drug
23 detecting dog, noting specifically that the dog’s performance in the field may be relevant.
24 *Florida v. Harris*, 133 S. Ct. 1050, 1057 (2013). “[C]ircumstances surrounding a particular
25 alert may undermine the case for probable cause” in some instances. *Id.* at 1057-58.

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

1 surveillance programs served as the “confidential source ... provid[ing] investigating agents
2 with ... new cellular telephone number[s]” of the targets of the investigation, Defs’ Exh. Q
3 (ECF No. 230) at Bates 01001350, so too is information about how these programs function.
4 And just as the “circumstances surrounding a particular alert” may undermine probable cause in
5 a dog sniff situation, *Harris*, 133 S. Ct. at 1057, the same is true of information about the
6 “algorithm and advanced search features” used by Hemisphere “to find the new number.” *See*
7 Hemisphere Slide Deck at 5. Indeed, the government acknowledges that the replacement phone
8 numbers identified by Hemisphere are only “ranked by probability.” *Id.* at 7. Under *Brady* and
9 Rule 16, the defense is entitled to information that would allow cross-examination over the
10 reliability of these surveillance programs.
11

12 Third, due process prohibits the government’s deliberate omission of information
13 necessary to bring a suppression motion. In *United States v. Barton*, 995 F.2d 931, 934 (9th Cir.
14 1993), the Ninth Circuit held that the deliberate destruction of evidence that would allow a
15 defendant to impeach the officer who submitted a search warrant affidavit violates “the due
16 process principles announced in *Brady*.” *Id.* at 935. *Barton* relied on *Franks v. Delaware*, 438
17 U.S. 154 (1978), which held that defendants have a right to challenge deliberately falsified
18 statements submitted in support of a search warrant application. *Barton*, 995 F.2d at 934-35.
19 The underlying rationale of both *Barton* and *Franks* is that “an officer” should not be permitted
20 to “feel secure that false allegations in his or her affidavit for a search warrant could not be
21 challenged.” *Barton*, 995 F.3d at 935; *see also Franks*, 438 U.S. at 168 (Fourth Amendment’s
22 probable cause requirement “would be reduced to a nullity if a police officer was able to use
23 deliberately falsified allegations to demonstrate probable cause, and, having misled the
24 magistrate, then was able to remain confident that the ploy was worthwhile”).
25

26 This same rationale prohibits the deliberate *omission* of information necessary for a
27 successful motion to suppress. *Cf. United States v. Stanert*, 762 F.2d 775, 780-81 (9th Cir.
28 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

1 reckless omissions of facts that tend to mislead.”). Here, publicly available evidence suggests
2 that law enforcement agents are intentionally omitting relevant information about their
3 investigations, even in “official document[s].” Hemisphere Slide Deck at 12 (“never refer to
4 Hemisphere”); *see also* “U.S. Directs Agents To Cover Up Programs,” *supra* note 8 (agents
5 directed to omit reference to NSA-derived information and instead “recreate” information
6 provided). An internal email from the U.S. Attorney’s Office *in this district* indicates that
7 federal agents were using stingray technology “without making that explicit” in pen register
8 applications to this Court. *See* Defs’ Exh. O (ECF No. 230) at 1. Due Process should prohibit,
9 and not reward, such intentional omissions, as they would allow the government to “feel secure”
10 that its reliance on unlawful forms of electronic surveillance “could not be challenged.” *Barton*,
11 995 F.2d at 935.
12

13 In sum, *Brady* and Rule 16 require disclosure of all of the sources of the cell phone data
14 obtained by the government in this investigation. This includes the sources of the 750,000 calls
15 identified on the spreadsheet produced to defendants and the “confidential sources” that
16 supplied new phone numbers. The Fourth Amendment right to be free from unconstitutional
17 electronic surveillance “would be reduced to a nullity” (*Franks*, 438 U.S. at 168) if the
18 government were permitted to conceal from Defendants and the Court factual information about
19 the extent to which the government relied on Hemisphere or other unconstitutional forms of
20 electronic surveillance to further the investigation.
21

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

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

28 “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

1 thought. But then again, they might not.” *In re Sealing and Non-Disclosure of*
2 *Pen/Trap/2703(d) Orders*, 562 F. Supp. 2d 876, 886 (S.D. Tex. 2008) (“*In re Sealing*”).²²
3

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

8 But the government goes to great lengths to keep its surveillance practices secret not
9 only from the public, but even from the courts. It takes affirmative measures to obscure its
10 reliance in criminal investigations on controversial surveillance sources, like Hemisphere or
11 NSA-derived intelligence, in documents presented to the Court. *See* Hemisphere Slide Deck at
12 12 (agents “instructed to never refer to Hemisphere in any official document”); “U.S. Directs
13 Agents To Cover Up Programs,” *supra* note 8 (Document obtained by *Reuters* directs agents to
14 omit reference to NSA-derived information from affidavits and courtroom testimony and to use
15 “normal investigative techniques to recreate the information provided”). Agents in this
16 district have apparently used stingray technology “without making that explicit” in
17 accompanying applications to this Court. *See* Defs’ Exh. O (ECF No. 230) at 1. Even in those
18 instances when the government sets forth its surveillance practices in applications for court
19 orders, the public has few methods for accessing this information.²³
20

21 ²² Judge Smith has identified a troubling phenomenon of permanently sealed electronic
22 surveillance dockets in district courts around country. Government applications for electronic
23 surveillance are typically filed under seal “until further order of the Court”; but because the
24 government rarely moves to unseal these orders, they typically remain sealed indefinitely. *See*
25 *id.* at 877-78; *see also* Stephen Wm. Smith, *Gagged, Sealed & Delivered: Reforming ECP’s*
26 *Secret Docket*, 6 Harv. L. & Pol’y Rev. 313, 322 (2012) (estimating that federal magistrate
27 judges issued more than 30,000 orders for electronic surveillance under seal in 2006, “more
28 than thirty times the annual number of [Foreign Intelligence Surveillance Act] cases”). Based
29 on the First Amendment and common law right of access to judicial records, Judge Smith
30 therefore announced that he would follow a new protocol, sealing electronic surveillance orders
31 only for six months, after which sealing orders would automatically expire absent a showing of
32 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

1 By keeping this information secret, the government, whether intentionally or not,
2 immunizes itself from popular, legislative, and legal challenges to its surveillance practices.
3 Because the government seeks court authorization – either statutory orders or probable cause
4 warrants – to engage in location tracking in *ex parte* proceedings, magistrates reviewing such
5 applications lack the benefit of the adversarial process in deciding these complex legal issues.
6 This has the potential to create serious distortions in the development of surveillance law, by
7 allowing the executive branch excessive authority in “making” the law.
8

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

15 //
16 //
17 //
18 //
19 //
20 //

21
22
23 by the United States’ Attorneys Office for the Northern District of California in this Court.
24 DOJ has asserted that it should not even have to search for records (let alone produce them)
25 because most of the records are under seal and it has *no* process for systematically ascertaining
26 “whether the conditions requiring sealing continue.” *See ACLU of Northern California v. Dep’t*
27 *of Justice*, N.D. Cal. Case No. 12-cv-04008-MEJ, ECF Nos. 43 at 18; 43-1 ¶ 9 (excerpts
28 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.

1
2 **III. CONCLUSION**

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

4 Dated: October 15, 2013

Respectfully Submitted,

5 By: /s/ Linda Lye
6 Linda Lye

7 Linda Lye
8 AMERICAN CIVIL LIBERTIES UNION
9 FOUNDATION OF NORTHERN CALIFORNIA
10 39 Drumm Street, 2nd Floor
11 San Francisco, California 94111
12 Telephone: 415-621-2493
13 Facsimile: 415-255-8437

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

16 Ezekiel Edwards (eedwards@aclu.org)
17 Nathan Freed Wessler (nwessler@aclu.org)
18 AMERICAN CIVIL LIBERTIES UNION
19 FOUNDATION
20 125 Broad Street, 18th Floor
21 New York, NY 10004
22 Telephone: 212-549-2500
23 Facsimile: 212-549-2654

24 Attorneys for *Amicus* American Civil Liberties
25 Union

26 Hanni M. Fakhoury
27 ELECTRONIC FRONTIER FOUNDATION
28 815 Eddy Street
San Francisco, CA 94109
Telephone: 415-436-9333
Facsimile: 415-436-9993

Attorneys for *Amicus* Electronic Frontier Foundation