JEFFRY GLENN, SBN 47357
BERMAN, GLENN & HAIGHT
5 Third Street, The Hearst Building
Suite 1100
San Francisco, CA 94103
Telephone: (415) 495-3950
Fax: (415) 495-6900
e-mail: SFLawyers@earthlink.net

Attorneys for Defendant:
FORTUNATO RODELO LARA

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. **FORTUNATO RODELO LARA,** Defendant.	Case No. 12-CR-0030-EMC Date: November 6, 2013 Time: 2:30 pm **NOTICE OF MOTION AND MOTION TO COMPEL DISCOVERY**

I.

NOTICE OF MOTION

PLEASE TAKE NOTICE that at an upcoming date and time to be selected by the court, Fortunato Rodelo Lara, by and through counsel, Jeffry Glenn will move this Court to enter an order directing the government to disclose evidence to the defense. The remaining co-defendants join in this motion, making it a joint defense request. The defendants will therefore jointly move the court to enter an order requiring the government to produce:

1. All exculpatory material and impeachment evidence in the possession of the San Francisco Police Department ("SFPD") and Office of Citizen Complaints ("OCC") relating to the officers and informants involved in this case pursuant to *Brady v.*

Maryland, 373 U.S. 83 (1963), *Giglio v. United States*, 405 U.S. 150 (1972), and *Kyles v. Whitley*, 514 U.S. 419 (1995). This includes:

a. Impeachment materials concerning the veracity of SFPD Officers Carl Bonner, Ricardo Guerrero, Britt Elmore, and any other officer who was the source of information included in the government's wiretap affidavits in this case, including information included in such officers' personnel files;

b. Impeachment materials regarding SFPD informants identified in the government's wiretap applications in this case as "CS-1," "CS-5," "CS-6," and "CS-7";

c. Any materials that tend to discredit representations made to the federal courts in the wiretap affidavits submitted in the case by SFPD Officer Bonner;

2. All call data obtained in this case, all phone numbers obtained/monitored in the course of this investigation, and all cell-site data obtained during the investigation.

3. Full documentation of the sources of all call record data collected by the government (including the San Francisco and Oakland Police Departments and the Northern California HIDTA Task Force) in this case, including data obtained (directly or indirectly) from cell phone service providers, the National Security Agency, the DEA Special Operations Division, the Hemisphere Project, the Northern California Regional Intelligence Center, or any other such government intelligence agency or task force group.

4. Any and all communications between law enforcement and/or Department of Justice officials involved with this case and the Hemisphere Project, the Northern California Regional Intelligence Center, or the DEA Special Operations Division, regarding the collection of cell phone call record data in the investigation of this case.

5. Any and all memos, records, expense reports, requisition forms, or other such documentation indicating any law enforcement officer involved in this or another

investigation used a device capable of intercepting a cell phone signal, including a "Stingray," "Triggerfish," WIT technology, ISMI capturer, or similar technology.

Defendants so move pursuant to the Due Process Clause of the Fifth Amendment and the Confrontation Clause of the Sixth Amendment to the United States Constitution and all other applicable case law and statutes set forth in the attached memorandum of law.

II.

STATEMENT OF FACTS

A. Pending Charges

On January 17, 2011, the U.S. Attorney's Office for the Northern District of California filed a fifteen-count indictment against twenty defendants, alleging various drug related offenses. All twenty defendants were charged in count one with conspiracy to distribute various controlled substances in violation of 21 U.S.C. § 846 and 841(b)(1)(A). Mr. Antonio Diaz-Rivera and Mr. Santos Cabrera-Arteaga were charged in counts two and three, respectively, with operating a Continuing Criminal Enterprise in violation of 21 U.S.C. § 848(a) (the 'CCE' charge). Counts three through fifteen charge various defendants with substantive drug possession and distribution defenses. All defendants initially entered pleas of not guilty.

B. Summary of investigation

It all began with a cell phone. In May 2008, the DEA task force agents obtained the cell phone number of Santos Cabrera-Arteaga, one of the two defendants in the case facing CCE charges. How the DEA got this phone number, however, is remarkably unclear. According to the government's affidavit in support of an application for GPS surveillance, filed under miscellaneous case number 09-CR-90331-MISC, the government "began analyzing telephone calls from CABRERA-Arteaga's primary cell phone numbers, which were obtained by a subject hereinafter referred to as a Source of Information ('SOI'). The SOI has been instrumental in identifying CABRERA-Arteaga and cellular telephone numbers associated with members of his DTO." The government did not further describe their

"Source of Information," nor has the prosecution disclosed any judicial order, subpoena or warrant that would account for the government's acquisition of Cabrera-Artega's phone records. They have also failed to turn over any call records from May or June of 2008 for *any* telephones despite the sworn affidavit stating that they relied on this information in building their case.

In August of 2008, DEA agents in Seattle received information from other unidentified "sources of information" that a group of Honduran nationals in Seattle with ties to the San Francisco Bay Area were distributing cocaine in the Seattle area. According to the sworn affidavit of the case agent in this matter, SFPD Officer Carl Bonner, after receiving this information from Seattle, "Agents analyzed toll records for cell phone numbers for these Honduran drug "runners" obtained from sources of information. Agents recognized links between these cell phone numbers and cell phone numbers used by members of the CABRERA-Arteaga DTO." Again, the government has not disclosed any judicial order, or subpoena, or search warrant that could account for the government's acquisition of these phone records – indeed, the oldest application for authorization to seize call detail records disclosed to the defense was filed on February 2, 2009.

Through a series of traditional law enforcement investigation techniques, DEA agents and local police in Seattle were able to identify an alleged drug distribution network comprised primarily of Honduran nationals and led by Mr. Jose Rodriguez-Rivera. Government agents eventually obtained wiretap authorizations for a number of telephones being used by members of this conspiracy, secured the cooperation of some of its members, and indicted 22 defendants in case number 12-cr-0021-JLR in the Western District of Washington. That case has since resolved for most or all defendants.

Back in San Francisco, local police and federal agents began working together under the supervision of a joint task force to investigate the case. Government agents used the information obtained from the Seattle case, along with a series of unidentified

'confidential sources,' to obtain court orders for pen registers,[1] allowing them to seize call data and cell-site location data[2] for multiple suspects, principally the two 'lead' defendants facing CCE charges: Mr. Diaz-Rivera and Mr. Cabrera-Arteaga. These pen registers orders,[3] which authorized the government to obtain cell-site data for every call and thus track the suspect's location every time he or she used a phone, were eventually expanded to cover phones allegedly used by many other suspects in the investigation. Using the call and cell site data derived from these pen registers, as well as information from unidentified 'confidential sources,' the government then obtained warrants for GPS data[4] for many of the targeted phones starting in 2009. This GPS information allowed government agents to constantly track the precise location of each individual, 24 hours a day, as long as they carried their cell phone with them.

Relying heavily on the fruits of their extensive electronic surveillance, including call records, location information, and cell-site information, the government eventually

---

A 'pen register' and 'trap and trace' device are pieces of physical equipment which in the past allowed law enforcement to track all incoming and outgoing phone calls from a particular number. In modern times, however, those records are kept by the phone company digitally and automatically, so the distinction between the two (like the actual hardware) is no longer meaningful. Use of 'pen register' devices to obtain call data is governed by 18 U.S.C. § 3121 *et seq* and § 2701 *et seq*.

All cellular telephones operate by communicating directly with cell towers, which connect the individual phone to a phone network, the internet, etc. Cell phone companies typically keep track of which cell phone tower an individual cell phone was/is communicating with when it places a call, as well as which direction from the tower. This information, referred to as 'cell site data,' can be used to locate and track an individual's location.

All of the pen register orders in this case sought and obtained permission to collect cell-site data without a warrant, a practice which several courts have found unconstitutional. *See In re Application of the United States*, 809 F.Supp.2d 113 (E.D.N.Y. 2011) (warrant required to compel disclosure of cell-site records); *In re Application of the United States*, 736 F.Supp.2d 578 (E.D.N.Y. 2010), rev'd No. 10-MC-0550 (E.D.N.Y. Nov. 29, 2011) (unpublished order noting written opinion to follow); see also *United States v. Jones*, 565 U.S. ___ (2012); *United States v. Maynard*, 625 F.3d 544 (D.C. Cir. 2010). The issue remains unresolved in the Ninth Circuit.

Phone companies are now required to collect 'precise' location information as part of E-911 requirements, either by GPS or satellite triangulation. Since GPS is by far the most common (and capable of locating a phone within just a few feet), the term GPS location is used in this motion.

obtained authorization for a wiretap of three cell phones believed to belong to Mr. Diaz-Rivera and Mr. Cabrera-Arteaga in January of 2010. A number of purportedly incriminating phone calls were recorded on those initial wiretaps. Using information from those recorded calls, the government sought extensions of the original taps and "spin off" wiretaps of new target phones, along with more pen register orders and GPS warrants. These subsequent wiretaps led to still more, until eventually 12 different wiretap orders were obtained leading to some 10,000 pages of 'pertinent' call information.

Many of the suspects repeatedly changed phone numbers during the investigation, but government agents displayed an uncanny ability to identify the new phone numbers almost immediately. Government agents then obtained pen registers, GPS warrants, and wiretap authorizations for these new phone numbers, often within days of them coming online. In its affidavits, the government has simply stated that these numbers were obtained through 'sources of information' which are not identified and 'common calling patterns' which are often not spelled out with any specificity.

Over the course of the investigation, the government augmented their electronic surveillance with some traditional law enforcement techniques, including traffic stops, physical surveillance, pole cameras at key locations, and the use of informants. The vast majority of the evidence in this case, however, is derived from electronic surveillance of the defendants' cell phones.

C. Scope of discovery produced thus far

Since the arrest of the defendants and the unsealing of the Indictment, the government has produced a tremendous quantity of discovery related to the investigation. These disclosures include over 1,200 pages of law enforcement reports, and an even greater number of photographs, DMV records, airplane travel records, and the like. This type of 'traditional' discovery, however, is dwarfed by the scope of electronic surveillance in this case. Electronic surveillance materials disclosed to the defense in this case include call data for over 700,000 phone calls, 12 different wiretaps in the Northern District alone resulting in 10,000 pages of transcripts of "pertinent" recorded telephone calls, and well

over 100,000 points of GPS-derived location data. *See* Exhibit R - Declaration of Counsel. The materials used to acquire this massive surveillance effort are also vast: some 4,000 pages of legal papers (applications, affidavits, and orders) in support of 69 pen register applications, 12 wiretaps, and dozens of GPS warrants have been disclosed to the defense thus far. *See id.*

As substantial as these materials are, they include only material derived directly from the investigation in the Northern District of California, and do not include the large number of materials derived from the closely interrelated Seattle and Los Angeles investigations. The government has provided several gigabytes of additional discovery related to the investigation in the Western District of Washington, as well as wiretap documents related to a state-court wiretap in Los Angeles directed at the suspected source of supply in Southern California.

III.

MOTION TO COMPEL PRODUCTION OF EXCULPATORY MATERIAL IN THE POSSESSION OF LOCAL LAW ENFORCEMENT

A. Introduction and summary of argument

The investigation in this case was conducted by a joint task force comprised of officers from the SFPD, Oakland Police Department ('OPD'), and DEA. Much of the investigative work was performed by state and local law enforcement, often by officers who were deputized federal agents. One such agent, SFPD Officer Carl Bonner, was the lead case agent and was the affiant for each wiretap application in the case.

Despite the central role of local law enforcement in the government's investigation – including the use of purported confidential sources who met only with local police – the U.S. Attorney has taken the position that they do not have a *Brady* duty to disclose exculpatory information which is currently in the possession of local law enforcement agencies, even where that evidence could discredit the local officers or their confidential informants who carried out the investigation. *See* Exhibit R.

This position, however, is not supported by Ninth Circuit law, which requires the federal government to actively obtain and disclose all exculpatory evidence from local law enforcement where the local law enforcement officers were acting as "agents" of the federal government. The defense therefore requests that this Court enter an order directing the U.S. Attorney to obtain and disclose all exculpatory evidence regarding the officers, informants, witnesses, or investigation of this case in the possession of local law enforcement.

B. The government relied heavily on SFPD officers who acted as 'agents' of the federal government

The government's affiant for each of the wiretap applications in this case was SFPD Officer Carl Bonner.[5] In the government's first application for wiretap authorization, filed on January 21, 2010, the Assistant U.S. Attorney who signed the application, Tarek Helou, swore to the reviewing court that he had "discussed all of the circumstances of the above offenses with Task Force Officer Carl A. Bonner of the Drug Enforcement Administration ('DEA'), *who has directed and conducted this investigation*." See Exhibit B at Bates 1000010 (emphasis added).

The "Task Force" to which AUSA Helou referred appears to be the "Metro Task Force Group," a joint federal, state and local narcotics task force that involves officers and agents from many state and federal law enforcement agencies in investigations of "drug trafficking organizations." See Exhibit A at Bates 1000033-34. According to the Northern District U.S. Attorney's Office, the particular task force investigation underlying

[5] The initial wiretap affidavit is filed herewith as Exhibit A. The defense has filed Exhibit A under seal as it contains extensive identifying information concerning numerous individuals not charged in this case. Exhibit B is the application for a wiretap authorization.

this case primarily involved "the Drug Enforcement Administration, Internal Revenue Service – Criminal Investigations, San Francisco Police Department, and Oakland Police Department," with additional investigation provided by more than a dozen state and federal agencies.[6]

In the affidavit the government submitted in support of the January 21, 2010, wiretap application, SFPD Officer Bonner described his various law enforcement assignments as follows:

> I am a sworn Federal Task Force Officer ("TFO") currently detailed to the San Francisco Drug Enforcement Administration ("DEA"). I am also an Inspector of Police assigned to the Investigative Bureau of the San Francisco Police Department ("SFPD") and I have been a sworn California Peace Officer for over 24 years.

Exhibit A at Bates 1000033-34; *see also* Bates 1000256 (Officer Bonner describing himself in a search warrant affidavit filed in federal court: "I am an Inspector of Police in the San Francisco Police Department. I am currently assigned as a Task Force Officer with the Drug Enforcement Administration."). Officer Bonner also noted he is "certified by the California State Attorney General's Office in the practical, technical, and legal aspects of court-ordered wiretaps." Exhibit A at Bates 1000034.

The first informant discussed in the Bonner Affidavit was "CS-1," who Officer Bonner indicated was a "tested confidential source for the SFPD" who had "received monetary compensation in this investigation from the SFPD." *See* Exhibit A at Bates 1000055 at n.22. According to the Bonner Affidavit, CS-1's supervisors in the investigation, who debriefed CS-1 and conducted a follow-up investigation regarding the informant's activities, included SFPD Officers Ricardo Guerrero and Britt Elmore. See *id.* at 1000065, 1000067 n.27, 10074, 1000106. Officer Guerrero also apparently supervised "CS-5," "CS-6," and "CS-7," the additional informants who provided information to the Task Force through Officer Bonner. *See id.* at Bates 1000111-114.

See Exhibit C, DOJ Press Release, available at: http://www.justice.gov/usao/can/news/2012/2012_01_26_20.defendants.indicted.press.html (all websites checked on date of filing)

According to the Bonner affidavit, CS-5 and CS-6, like CS-1, were "tested confidential source[s] for the SFPD. . ." *Id.* at Bates 1000111 n.48, 1000113 n.49.

In sum, the pre-wiretap investigation of the case was directed by SFPD officers and was driven by information supplied by SFPD informants.

By May of 2012, after the Indictment issued, Officer Bonner was still directing the investigation of the Diaz-Rivera organization. According to DEA reports of debriefings disclosed to the defense within the past month, one defendant engaged in a post-arrest proffer session with counsel for the government and several agents, including Officer Bonner. The report makes clear that officer Bonner took the lead in questioning the potential cooperator. *See* Exhibit D – Debriefing reports.

On July 30, 2013, the same defendant again engaged in a debriefing with the government. The DEA report of this debriefing, which was prepared by DEA Special Agent Kristopher Sullivan, noted Officer Bonner was present during the interview and "that TFO Officer Carl A. Bonner of the San Francisco Police Department authored the DEA-6 as the case agent in this investigation." *See* Exhibit D. Once again, the report plainly indicates Officer Bonner took the lead in debriefing the cooperator.

C. The SFPD was an integral part of the Diaz-Rivera investigation and the government's *Brady* obligation therefore extends to materials in the possession of the SFPD.

The U.S. Attorney for this district has asserted that for the purposes of discovery, state and local agents who participate in joint task force investigations should be considered agents of the federal government. *See United States v. Fort*, 472 F.3d 1106 (9th Cir. 2006). In *Fort,* the Ninth Circuit described the government's position:

> [W]e are still left to determine who qualifies as an "agent" of the federal government in the context of the discovery process in a federal criminal prosecution. ... the government urges that the term "government agent" be given a broader definition that would **include state or local police officers whose investigation of a defendant provides evidence to support a federal prosecution** of the same defendant for the activities so investigated.

Id. at 1111 (emphasis added).

The *Fort* court concluded that the phrase "government agent," in the context of the federal rules of criminal procedure, "includes non-federal personnel whose work contributes to a federal criminal 'case.'" *Id.* at 1113. The court further held that the phrase "in connection with investigating or prosecuting the case," is so broad as to include any such work by any "government agent," at any time, even before there is a federal case. *Id.* at 1119-20. This combination of rulings transforms local police officers involved in local investigations before any federal prosecution was even contemplated into federal "government agents." *Id.*

Writing in dissent of the denial of *en banc* review in the *Fort* case, Judge Wardlaw, joined by five Ninth Circuit judges, interpreted the panel's holding as a significant expansion of the government's *Brady* obligations:

> The extension of *Brady* to knowledge not personally held by the prosecutor has been driven by theories of government agency. *See Giglio, 405 U.S. at 154* (applying agency principles to prosecutors as spokesmen for the federal government). As noted previously, *Rule 16* and *Brady* are in many ways two sides of the same coin. If a local agency is a "government agent" for *Rule 16* purposes, it should also be deemed an agent for *Brady* purposes. This extends the federal government's *Brady* duties to include information in the control of local agencies that participated in the "case."

United States v. Fort, 478 F.3d 1099 1105-06 (9th Cir. 2007) (Wardlaw, J., dissenting).

When federal and state agencies cooperate extensively on a joint investigative task force, the state agencies may be deemed to be "agents" of the federal government such that their knowledge of exculpatory information should be imputed to federal prosecutors. *See United States v. Antone*, 603 F.2d 566 (5th Cir. 1979) (state investigators were deemed to be agents of the federal prosecution team for the purposes of *Brady* when "the two governments, state and federal, pooled their investigative energies to a considerable extent"); *United States v. Leos-Harmosillo*, 213 F.3d 644, 2000 WL 300967 (9th Cir. 2000) (unpublished) (*Brady* information possessed by state police officers was attributed to the prosecutors when the officers were acting on the federal government's behalf and subject to its control). As Judge Alsup of this district recently noted in another joint task

force case, "[w]here . . . the federal prosecutors have state police working on their behalf, it seems clear that the reasoning of *Kyles* requires federal prosecutors 'to learn of any favorable evidence known to *others acting in the government's behalf*,' including any local police acting on its behalf in the investigation." *United States v. Cerna*, 633 F. Supp. 2d 1053, 1059 (N.D. Cal. 2009)(emphasis original).

Here, there is no question that several SFPD officers were acting as "agents" of the federal prosecutors as part of the investigation into the so-called "Diaz-Rivera Drug Trafficking Organization." The U.S. Attorney's Office identified SFPD Office Bonner as the agent who "directed" the investigation, and Officer Bonner swore out each of the government's wiretap affidavits. Moreover, much of the investigation described in Bonner's affidavits was the work product of SFPD officers and the informants they supervised. *See* Exhibit A. Defendants submit that in this case, not only were SFPD officers acting as "agents" of the federal prosecutors, Officer Bonner was the "lead investigative agent" in the Task Force investigation.

In *United States v. Price*, 566 F.3d 900 (9th Cir. 2009), the government prosecuted a felon in possession case based on a traffic stop and search of the defendant conducted by the Portland Police Department, and presented crucial testimony at trial from an informant controlled by the Portland PD. *Id.* at 902. Though the informant had a long criminal history of fraud and deceit, counsel for the government did not disclose the informant's criminal record to the defense. *Id.* at 903. Counsel for the government indicated he did not turn over the informant's criminal history because he did not personally possess the materials, though the materials were obviously available to the Portland PD. *See id.*

The Ninth Circuit found the government's "personal possession" argument missed the point and that "the prosecutor utterly failed in his '*duty to learn* of any favorable evidence known to the *others* acting on the government's behalf in the case, including the police.'" *Id.* at 9803 (citing *Kyles v. Whitley,* 514 U.S. 419, 437 (1995))(emphasis original). The Court went on to hold:

> Under longstanding principles of constitutional due process, information in the possession of the prosecutor *and* his investigating officers that is helpful to the defendant, including evidence that might tend to impeach a government witness, must be disclosed to the defense prior to trial. . . Because, here, the prosecutor failed to fulfill his duty to learn of and disclose favorable evidence that likely was in the possession of his lead investigating officer . . . we hold that the prosecutor violated Price's rights under *Brady v. Maryland* .

Id. at 903; *see also Cerna,* 633 F.Supp 2d at 1059 (citing *Price* for the rule that "despite the separate sovereignty concept, two alternative avenues can lead to a *Brady* duty in the federal-state context. The first is when the federal prosecutor uses a state or local officer as a "lead investigating agent").

Officer Bonner was the "lead investigating agent" for the government in this case. According to the government, Officer Bonner "directed" the investigation and his wiretap affidavits make clear that he coordinated the flow of information from SFPD officers and their informants to the joint task force. Even after the Indictment issued, Officer Bonner continued to lead the government's debriefings of informants, and the DEA agents involved in the investigation continued to identify Officer Bonner as the Task Force "case agent."

In light of the central role SFPD officers played in this investigation, as well as the above precedents and the prosecution's arguments in the *Fort* case, the U.S. Attorney should be deemed responsible for disclosing all exculpatory materials in the possession, custody or control of the SFPD.

D. Due process requires that the prosecution diligently seek out exculpatory information in the possession of the SFPD.

As the above cases repeatedly note, the Supreme Court recognized in *Kyles v. Whitely*, 514 U.S. 419 (1995) that the prosecutor has personal duty to become aware of, and disclose, material exculpatory information. "[T]he individual prosecutor has a duty to learn of any favorable evidence known to the others acting on the government's behalf in the case, including the police." *Id.* at 437. In *United States v. Alvarez*, 86 F.3d 901 (9th

Cir. 1996), the Ninth Circuit reiterated the prosecutor's obligation to divulge impeachment information in the possession of cooperating police agencies. In that case the Ninth Circuit found that due process required the U.S. Attorney in charge of the federal prosecution to review the rough surveillance notes of Anaheim Police Department officers who participated in the investigation, and to turn over to the defense those portions of the notes that were facially exculpatory. *See id.* Clearly, where local police departments are an integral part of a joint federal/state/local investigation, the prosecutor has a duty to discover and make known to the defense all material exculpatory evidence. "Because the prosecution is in a unique position to obtain information known to other agents of the government, it may not be excused from disclosing what it does not know but could have learned." *United States v. Blanco*, 392 F.3d 282, 388 (9th Cir. 2004) (quoting *Carriger v. Stewart*, 132 F.3d 463, 480 (9th Cir. 1997) (en banc)).

Moreover, the Ninth Circuit plainly recognizes the import of producing complete *Brady* materials in each case. For example, in *Blanco*, the Ninth Circuit analyzed the "standard form" discovery promises by the U.S. Attorney's office of the District of Nevada, which expressly extends the government *Brady* disclosure obligations "*to evidence which is known by the Government counsel or which could become known by the exercise of due diligence.*" *Blanco*, 392 F.3d at 388 (emphasis in original). But the Ninth Circuit found that this standard form "misstated" the government's *Brady* obligations by understating them, and determined that simply "asking" for these materials is not enough and that the promise of *Brady* requires government counsel to obtain Brady information, even from recalcitrant agencies. *Id.* at 393-94; *see also Price*, 566 F.3d at 908 ("reliance on the prosecutor's lack of personal knowledge of the *Brady* material demonstrate[s] a clearly erroneous understanding of the law . . .").

The Ninth Circuit's decision in *United States v. Hanna* is also instructive on this issue. There, the Ninth Circuit, relying on *Kyles*, found that the federal prosecutor should have found and disclosed prior inconsistent statements contained in a SFPD file relating to

an officer involved in the arrest of the defendant. *United States v. Hanna*, 55 F.3d 1456, 1461 (9th Cir. 1995).

In *Hanna* the defendant was charged with a "trigger lock" offense by the U.S. Attorney for the Northern District of California. *Id.* at 1458. The charges resulted from an arrest and search of the defendant conducted by an officer of the SFPD. *Ibid.*

The arresting officer was one SFPD Sergeant Kitt Crenshaw, who prepared an incident report regarding the search and arrest. *Id.* at 1459. Before the federal grand jury, an ATF agent named Dios testified to a version of the arrest and search that differed from the SFPD Incident Report. *Id.* At trial, Sergeant Crenshaw testified to a third version of events leading up to the search of defendant Hanna. *Id.*

On appeal defendant Hanna complained that the federal prosecutors had failed to disclose the contradictory statements by Officer Crenshaw, as recorded in his SFPD Incident Report (and perhaps statements to Sergeant Crenshaw's commanding officer at the SFPD). *Id.* The Ninth Circuit agreed that the federal prosecutors were obligated to review the records of the SFPD in order to find any *Brady* material concerning the differing versions of the search:

> We do not suggest that any conceivable person acting on the government's behalf is deemed someone the government must seek out and interview . . . Here, however, concrete evidence exists in the record that San Francisco Police Department policy required officers to search prisoners immediately before placing them in a transportation vehicle, and that Sgt. Crenshaw submitted his report of this incident to his Lieutenant for approval. These facts, combined with the obvious discrepancies between Sgt. Crenshaw's report and his trial testimony, the substance of which the prosecutor presumably knew prior to trial, make it likely that the prosecutor knew that Sgt. Crenshaw may have made statements to his Lieutenant; and therefore, the government should have inquired about them.

Id., at 1460-61. Clearly, where local police departments are an integral part of a joint federal and state investigation, the prosecutor has a duty to make a diligent effort discover and make known to the defense all exculpatory evidence maintained by members of the participating local police agencies.

Allowing the government to erect a discovery barrier frustrates the guiding principles underlying *Kyles* and *Brady*, that the government has an obligation to ensure that a defendant receives a fair trial. In this case, the U.S. Attorney is on notice that a wealth of exculpatory material may exist in files in the possession of a local police agency that extensively participated in the government's investigation, yet the prosecution disavows any responsibility to review those files, despite the prosecution's decision to have SFPD officers spearhead the government's investigation. To allow the government to use SFPD informants and investigators as a sword in the task force investigation, but then shield those same sources from meaningful review by a prosecutor for *Brady* information, would utterly defeat the Due Process protections upon which the rule from *Kyles* rests. In *Price*, the Ninth Circuit was acutely aware of the problem inherent with such artificial barriers between the investigating law enforcement officers and the prosecutors who utilize the investigators' information in court when the court noted:

> Just as it "would undermine *Brady* [to] . . . allow [ ] the prosecutor to tell the investigators not to give him certain materials unless he asked for them," *Blanco, 392 F.3d at 388* (quoting *Zuno-Arce, 44 F.3d at 1427*), it would equally undermine *Brady* for a prosecutor to direct his investigator to perform an investigation and then fail to discover the investigation's full results.

Price, 566 F.3d at 909.

E. Conclusion

The SFPD is presently, and was at the time of the investigation of this case, joined in a task force with federal and local law enforcement agencies that functions under the supervision and control of the U.S. Department of Justice. This task force supervises the investigation and prosecution of a wide range of narcotics investigations in Northern California. As part of this task force, the local police agencies generated and maintained much of the evidence in this case. The Department of Justice has chosen to prosecute this case under the purview of the federal task force. When local law enforcement agencies take part in such joint task forces, and commit their officers and informants to key roles in investigations under the control of the U.S. Attorney's Office, the Court should not allow

the government to disclaim control over exculpatory information held in the files of any agency participating in the task force.

IV.

MOTION TO COMPEL SOURCES OF ELECTRONIC SURVEILANCE

A. Introduction and summary of argument

This case involves an exceptional amount of electronic surveillance, even for a federal wiretap case. The sources of much of the electronic surveillance obtained by the government in this case, however, remain shrouded in secrecy. The overwhelming majority of the call data obtained by the government in this case cannot be tracked to a valid court order, subpoena, or warrant that would permit the government to obtain it. Furthermore, the government's uncanny ability to 'locate' new cell phones used by suspects in the case is made particularly troublesome by the inconsistency and vagueness of their descriptions of how these phone numbers were obtained.

At the same time, recent revelations of the extensive yet well-concealed use by federal law enforcement officials of surveillance information obtained through potentially unconstitutional sources have raised serious questions about the limits of government power and the right to due process of law. The nation has learned that the National Security Agency ('NSA') has been secretly spying on every American by obtaining and recording call data for every phone call made in the United States and have been routinely turning this information over to law enforcement agencies. Similarly, cell phone service providers have joined operational groups, such as the Hemisphere Project and the Northern California Regional Intelligence Center, with the DEA and other law enforcement agencies for the express purpose of funneling decades of call records data to law enforcement agents in narcotics cases. We have also learned that right here in the Northern District of California, federal task force agents have regularly made use of "stingray" machines which directly intercept cell phone signals and can therefore be used to identify phone numbers, locate suspects, and even listen in on phone calls – all without judicial authorization. Most troubling of all, we have learned that the executive branch

has undergone extensive efforts to conceal this information from the public, and from the judiciary.

Based on the discovery received thus far, the defense believes that the government's investigation was aided by information derived from the NSA's secret spying program, or the Special Operations Division ('SOD') of the DEA, which obtains information from the NSA's secret domestic spying program and uses it to aid domestic law enforcement investigation, or the Hemisphere Project and the Northern California Regional Intelligence Center, or, perhaps most likely, from several of these sources. The defense also believes that the investigating officers and agents in this case used "stingray" or similar technology to wirelessly intercept cell phone transmissions of suspects in the investigation. The defense believes the government has failed to disclose any of this information to defense counsel or the Court, despite promises by the Department of Justice that they are obliged to do so.

The defense therefore moves this Court for a series of orders directed at not only the U.S. Attorney, but also the investigatory agencies and task force agents involved in the case, to disclose to the Court and to defense counsel the full extent of electronic surveillance conducted of the defendants.

B. The government has a *Brady* obligation to disclose any information which might aid the defendants in a motion to suppress the wiretap evidence

The government's *Brady* obligations require it to disclose to the defense any evidence which might aid in a dispositive motion to suppress evidence, and to provide this evidence in a timely fashion so that the defense has an opportunity to use that information in a pretrial motion to suppress or dismiss. While the constitutionality of using stingrays or surreptitiously and extra-judicially gathered cell phone data to obtain warrants in criminal cases has not yet been determined,[7] concealing that evidence from the defense

[7] *See United States v. Rigmaiden*, 2013 U.S. Dist. LEXIS 65633. (D.Ariz. 2013). the lone case in which the legality of a Stingray has ben litigated. Counsel is unaware of any case in which the legality of using NSA intercepts in domestic law enforcement has been

and the courts deprives defendants of due process of law by preventing them from presenting a suppression motion based on a claim that the evidence used to obtain the warrant constituted the fruit of the poisonous tree. As explained below, the government's investigation and wiretap applications relied heavily on electronic surveillance, and the sources of that surveillance must therefore be disclosed in a timely manner so that the defense is assured a fair chance to challenge the admissibility of the wiretap evidence.

The Ninth Circuit has specifically held "that the due process principles announced in *Brady* and its progeny must be applied to a suppression hearing involving a challenge to the truthfulness of allegations in an affidavit for a search warrant." *United States v. Barton*, 995 F.2d 931, 935 (9th Cir. 1993); *see also United States v. Tham*, 884 F.2d 1262, 1266 (9th Cir. 1989) ("Evidence is material only if there is a reasonable probability that, had the evidence been disclosed to the defense, the result of the proceeding would have been different."); *United States v. Veras*, 51 F.3d 1365, 1375 (7th Cir. 1995)(noting that *Brady* discovery is material if such discovery could have "affected the outcome of the suppression hearing", and thereby the case.); *Smith v. Black*, 904 F.2d 950, 966 (5th Cir. 1990) ("The appropriate assessment for *Brady* purposes, of course, is whether nondisclosure affected the outcome of the suppression hearing"), vacated on other grounds, 503 U.S. 930, 112 S. Ct. 1463, 117 L. Ed. 2d 609 (1992); *Indelicato v. United States*, 106 F. Supp. 2d 151, 159, 2000 U.S. Dist. LEXIS 10516 (D.Mass. July 19, 2000) (discussing standard for habeas relief on allegation that government suppressed *Brady* material relevant to defendant's motion to suppress wiretap evidence.).

In the unpublished case *United State v. Forcelledo,* the Ninth Circuit explained that due process can require pre-trial production of materials that might exculpate a defendant through a motion to suppress:

> Forcelledo claims that the various FBI reports were material because they would have enabled him to effectively challenge the government's contention that its wiretap application was proper. Forcelledo claims that he could have used the FBI

litigated, probably because that information is withheld from the judicial system as described below.

> reports to show that the government's wiretap application contained material omissions.
>
> If the FBI reports contained information that helped to establish that the government's affiant had misled the court when the affiant submitted the wiretap application, that information would have been material to the proceeding. Under Brady, Forcelledo would have been entitled to the reports. The district court reviewed the FBI reports in camera and determined that none of them contained material information. Our review of them satisfies us that the court did not abuse its discretion.
>
> *United States v. Forcelledo*, 1990 U.S. App. LEXIS 20433 (9th Cir. 1990).

C. The government relied heavily on electronic surveillance data in obtaining authorization for the wiretaps

The initial affidavit of DEA Task Force and San Francisco Police Officer Carl Bonner that the government submitted in support of its wiretap applications in this case ("the Bonner Affidavit") reveal that this was not an ordinary wiretap investigation, at least in terms of the government's reliance on cell phone data. The affidavit only minimally relied on the usual phone contacts between the targets and informants or undercover agents. Instead, the Bonner Affidavit resorted to a complex analysis of massive amounts of cell phone and GPS data to both establish which phones were being used by which targets and to link those phones to suspicious activity on the part of the suspects.

The Bonner Affidavit began by noting the government had relied on oral and written reports from DEA agents and agents of other federal agencies, as well as "[r]eviews of pen register, trap and trace and telephone toll record information" and "information describing the physical location of the Target Telephones and other telephones, including predecessor phones of the Target Telephones. This information includes latitude and longitude information, GPS data, E-911 Phase II data, and cell-site data, and gives agents the precise location of the cellular phone being monitored." Bates 1000042.[8]

[8] The affidavit noted the government "began monitoring the precise location of cellular telephones linked to the CABRERA-Arteaga" on May 22, 2009, and that "[s]ince that time, precise location data monitoring, in conjunction with physical surveillance and phone toll analysis, has been on-going in this investigation." Bates 10000133. The affidavit was submitted on January 221, 2010, by which time the government had been

The Bonner Affidavit then indicated all of these "Target Telephone" facilities had been identified through the government gathering and analysis of cell phone data:

> Agents have identified ten cell phones, in addition to Target Telephone 1, that they believe Santos CABRERA-Arteaga has used to facilitate drug trafficking. One predecessor phone of Target Telephone 1 was linked to drug seizures on April 30, 2009 and June 1, 2009. On September 12, 2009, agents obtained additional evidence of Santos CABRERA-Arteaga's using Target Telephone 1 to facilitate drug trafficking. On that date, agents watched Santos CABRERA-Arteaga on a pole camera as he used a cell phone while apparently creating hidden compartments in a car that could be used to store drugs or drug proceeds. **Pen register data showed that Target Telephone 1 was being used at the same time, and precise location monitoring showed that Target Telephone 1 was at the very location where Santos CABRERA-Arteaga was observed with the pole camera. While Santos CABRERA-Arteaga was using Target Telephone 1, he called a predecessor phone of Target Telephones 2 and 3, which agents believe was used by Antonio DIAZ-Rivera, the leader of the DIAZ-Rivera DTO.**
>
> Target Telephones 2 and 3 are identified in Paragraph Six. Agents believe that DIAZ-Rivera uses Target Telephones 2 and 3 to facilitate drug trafficking of the DIAZ-Rivera DTO. **Agents have identified 11 additional phones that they believe have been used by DIAZ-Rivera in a similar fashion, with similar calling patterns and similar common callers to Target Telephones 2 and 3. The common callers included suspected drug traffickers. Additionally, since agents began focusing on Target Telephones 2 and 3 and their predecessors, they have monitored the precise location of seven of these phones, including Target Telephones 2 and 3. The precise location monitoring showed that all seven of these phones were present at 244 University Street in San Francisco at times and for durations that support the conclusion that the user of the phone lives there** (e.g., present at night and remaining there until the following morning). Agents have seen DIAZ-Rivera at that address three times and believe that he lives there. For example, on June 9 and 10, 2009, agents observed DIAZ-Rivera: go from his suspected residence at ... to San Francisco International Airport; board a flight to Seattle; land in Seattle, where he went directly to the residence of suspected co-conspirator Jose RODRIGUEZ-Rivera; drive to within one block of the apartment of a drug dealer arrested for selling cocaine and methamphetamine later that day; fly back to San Francisco; and return he landed. **Cell-site data from TT2 Predecessor 7, which agents believe DIAZ-Rivera was using at that time, confirmed that the phone went to Seattle and returned to San Francisco at times matching DIAZ-Rivera's surveilled travel.**

---

gathering detailed cell phone records of the targets for more than a year, and GPS data for eight months. Oddly, this affidavit makes no mention of obtaining call data for the Cabrera-Arteaga phone in May 2008 as disclosed in other affidavits.

> Agents believe that DIAZ-Rivera is using Target Telephones 2 and 3 to traffic drugs because: a. DIAZ-Rivera and **predecessor phones of Target Telephones 2 and 3 were linked to drug seizures in January 2009 and June 2009;** b. On September 12,2009, agents saw Santos CABRERA-Arteaga **use Target Telephone 1 to call a predecessor of Target Telephones 2 and 3 while Santos CABRERA-Arteaga disassembled car doors** in a manner consistent with installing hidden compartments that could be used to transport drugs or drug proceeds; c. A **predecessor of Target Telephones 2 and 3 was linked** to an attempted purchase of cocaine by an undercover agent in October 2009; and d. **Phones that agents believe DIAZ-Rivera used before Target Telephones 2 and 3 were in contact with other phones that have been intercepted conducting drug transactions on wiretaps in other investigations.**
>
> Bates 1000051-53 (emphasis added).

Agent Bonner went on to describe how the DEA linked the targets to a group of Honduran nationals under investigation in Seattle. Again, the analysis in the affidavit was almost wholly dependent on cell phone data:

> After conducting those interviews in Seattle, agents discovered links between the CABRERA-Arteaga DTO and another organization, later identified as the DIAZ-Rivera DTO. The DIAZ-Rivera DTO appears to be a well-organized DTO with narcotics trafficking links to California, Washington, Texas, Canada, and Culiacan, Tijuana and Michoacan, Mexico. It is comprised largely of El Salvadoran nationals in the San Francisco Bay Area and in the Seattle metropolitan area. **Phone toll analysis, physical surveillance, precise location information, pole cameras, and links to other DEA investigations** led agents to believe that the following El Salvadoran nationals are members of the DIAZ-Rivera DTO: Antonio Jose DIAZ-Rivera, Jose Anibal RODRIGUEZ-Rivera, Fatima SEGOVIA, Jose Anibal VARGAS-Sierra, Dennis Leonel ALMENDAREZ (who may be a Mexican national), Marcos Antonio FLORES, Carlos BUSTILLO-Zavala (a/k/a Carlos ZAVALA-Bustillo), other Interceptees, and others not yet identified. Agents believe that the second DTO is controlled by Antonio Jose DIAZ-Rivera.
>
> Agents believe that the two DTOs may work together to distribute drugs. For example, agents **monitoring the precise location of Target Telephone 1,** used by Santos CABRERA-Arteaga, learned that it went to DIAZ-Rivera's residence on August 21, 2009, the same day that agents made a ruse call to, Target Telephone 1 and observed Santos CABRERA-Arteaga use it. Additionally, both DTOs were linked to a June 2009 seizure of 7 kg of cocaine and 8 pounds of methamphetamine discussed in Paragraphs 46-47 and 79-93. Furthermore, members of the two DTOs **have been in telephone contact with each other,** including an October 24, 2009 three-way call between a predecessor phone of Target Telephones 2 and 3, and phones that agent believe are used by TOBAR-Galdamez, a suspected courier for the CABRERA-Arteaga DTO, and RODRIGUEZ-Rivera, the suspected leader of the DIAZ-Rivera DTO's Seattle cell.

Bates 1000058-59 (emphasis added).

Regarding the primary target of the investigation, defendant Santos Cabrera-Artega, the Bonner Affidavit again indicated the primary basis for probable cause as to Cabrera-Arteaga's cell phone was analysis of cell phone data:

> Agents have reviewed information from confidential sources, **links to other investigations, call frequency counts, common calling patterns, physical surveillance, and precise location monitoring.** _Based on that information, agents believe that Santos CABRERA-Arteaga has used each of the phones identified in Chart I, below. _Agents believe that those phones are the predecessor phones of Target Telephone 1.

Bates 10060 (emphasis added).

The affidavit proceeded to give the court a 36-page summary of how the agents used call record, cell site and GPS data to monitor the activities of Mr. Cabrera-Arteaga and his suspected associates. *See* Bates 1000061-97. While this description of the suspects' activities did include some contacts with informants and undercover agents, the vast majority of the government's showing of probable cause relied on cell phone data and surveillance. *See id.*

E. The government must disclose the sources of all call data it obtained in this investigation

i. Discovery provided thus far cannot account or provide judicial authorization for the government's far-reaching surveillance.

The government has provided defense counsel with a single spreadsheet which purportedly contains all call data obtained in the course of this investigation. This document, Bates No. 4001255, contains call data for 742,907 phone calls.[9] *See* Exhibit R. For each call, the spreadsheet provided by the government lists the 'target' phone number, number dialed or dialing in, date, time, and duration of the call, and – in some cases – the

[9] The call data is too voluminous to be filed as an Exhibit for the purposes of this motion, though it can be made available to the court.

cell tower and direction at the start and end of the call.[10] While the actual phone numbers are provided for most of these calls, a substantial number have only UFMI, ISMI, or other unique identifying numbers for the phones used rather than an actual phone number. In some cases, a formatting error has destroyed even the UFMI/ISMI number, making identification of the phone impossible. *See* Exhibit R.

A rudimentary analysis of these three-quarters of a million phone calls reveals that at least 643 different phone numbers are listed as 'target' phones. *See* Exhibit R. This would seem to indicate that the government obtained court orders allowing them to gather records for a staggering 643 different telephones – otherwise there is no way they could have (legally) obtained the call data for those phones. In discovery, however, the government has produced just 69 court orders authorizing the government to obtain call record data for only 52 different phone numbers.[11] In short, the government has produced orders allowing the collection of call data for 52 phones, but actually collected call record data for several hundred.

Naturally, this begs the question of how the government obtained all of these phone records. When asked, the AUSA on the case indicated he believed the phone records to have been obtained by "administrative subpoena." Federal law, however, prohibits the acquisition of such call data without a court order or warrant. *See* 18 U.S.C. § 3121(a) ("Except as provided in this section, no person may install or use a pen register or a trap and trace device without first obtaining a court order under section 3123 of this title or under the Foreign Intelligence Surveillance Act of 1978"); 18 U.S.C. § 2701 et seq. (the Stored Communications Act); 18 U.S.C. § 2703(a) ("A governmental entity may require the disclosure by a provider of electronic communication service of the contents of

---

[10] Oddly, even though each of the court orders disclosed in this case authorize the government to acquire cell-site data from the service providers, the cell-site information is provided for a relatively small minority of phone calls. It is unclear whether this information was withheld from the spreadsheet disclosed or whether it was not obtained in the first place.

[11] 17 of the orders contain repeated phone numbers.

a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant..."); 18 U.S.C. § 2703(c) ("A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity - (A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . . by a court of competent jurisdiction; (B) obtains a court order for such disclosure under subsection (d) of this section . . .")

ii. The government is obliged to disclose the source of its evidence

The non-disclosure of pen register orders is not a new phenomenon. According to a 2012 article by Magistrate Judge Stephen Smith, the government obtains tens of thousands of sealed surveillance orders every year, and they remain under seal without any scrutiny from defense counsel or the appellate courts. *See Gagged, Sealed, & Delivered: Reforming ECPA's Private Docket*, 6 Harv. L. & Pol'y Rev. 313, 321 (2012). In this case, however, the government has purportedly disclosed all of its pen register orders and applications. If the government did not obtain these voluminous call detail records by court order or search warrant, that would indicate they obtained them from a database source such as NSA, the DEA Special Operations Division, or the Hemisphere Project. In any event, defense counsel has a right to know where the evidence was obtained so that they can determine whether the evidence was illegally obtained and potentially subject to suppression. There is no way for defense counsel to properly assess the legality and admissibility of the government's evidence – including the wiretaps – without first determining whether the information used to obtain that wiretap was acquired in compliance with the Constitution and Federal law. Since, as explained above, the GPS and wiretap authorizations relied very heavily on call data, due process requires that defense counsel be given a full and fair opportunity to assess the legality of this

information. Withholding the source of this information while disclosing the information itself is akin to introducing evidence seized via search warrant without providing a copy of the warrant itself and accompanying affidavit. That, of course, would be prohibited. *C.f. United States v. Bus. of Custer Battlefield Museum & Store Located at Interstate 90, Exit 514, S. of Billings, Mont.*, 658 F.3d 1188, 1192 (9th Cir. 2011) (holding that individuals have a common law right to access search warrant materials, even if no charges are filed).

iii. The Government has engaged in wide-ranging secret surveillance only recently discovered by the public

On June 5, 2013, *The Guardian* and several other publications broke the story that the NSA had ordered Verizon[12] to transmit, on an ongoing basis, all of the phone records of every telephone in its systems, whether within the United States or without. See Exhibit E - NSA collecting phone records of millions of Verizon customers daily, The Guardian, June 5, 2012.[13] A copy of the FISA order itself is attached as Exhibit F. This information was leaked to the press by Edward Snowden, a former NSA security contractor turned whistleblower, who went on to reveal that the NSA had in fact long been secretly collecting the phone records of every American. See Exhibit G – NSA violated court rules on collecting phone call data, Washington Times, Sept. 10, 2013.[14] The FISA court had secretly condoned this practice on the grounds that the Supreme Court had previously held in *Maryland v. Smith*, 442 U.S. 735 (1979), that individuals did not have a reasonable expectation of privacy in the numbers they dialed. See Exhibit H - FISA Order. This is despite the fact that the Supreme Court has much more recently indicated that the 'third-party' doctrine on which *Smith* was based is likely no longer applicable in

[12] Verizon is one of the largest telecommunications companies in the United States.
[13] Availalble at: http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order
[14] Available at: http://www.washingtontimes.com/news/2013/sep/10/nsa-violated-court-rules-on-collecting-phone-call-/?page=all

today's digitally interconnected world. *See United States v. Jones*, 565 U.S. ___, 132 S.Ct. 945 (2012).

Subsequent revelations indicated that the NSA had also collected vast numbers of private emails and internet use activity without prior judicial authorization, obtaining some 1-2 *billion* records per day. *See* Exhibit I – XKeyscore: NSA tool collects 'nearly everything a user does on the internet,' The Guardian, July 31, 2013. These systems, according to Snowden and confirmed by materials he provided, allowed him almost limitless power to spy on anyone's electronic communications. "'I, sitting at my desk,' said Snowden, could 'wiretap anyone, from you or your accountant, to a federal judge or even the president, if I had a personal email.'" *See id.*

iv. The government has broken its own promise to the judicial branch to disclose this surveillance to defendants.

The government has explicitly promised that any FISA intercepts used in criminal cases would be disclosed to the defense. On October 29, 2012, Solicitor General Donald Verrilli, speaking on behalf of the Department of Justice, argued before the Supreme Court in *Clapper v. Amnesty International*, 133 S.Ct. 1138 (2013) that individuals – including lawyers, journalists, and human rights activists – whose information was obtained by the NSA's surveillance program lacked standing to challenge that surveillance unless the government provided notice to them that information obtained from such surveillance was to be used in a criminal case against them. During oral argument, the Solicitor General told the Supreme Court that if the government was going to use evidence obtained under the FISA Amendments Act ('FAA'), the source of that information would have to be disclosed. See *id.*, at 1154. The Supreme Court held, in light of this notice requirement that the plaintiff's in the case lacked standing to challenge the FISA intercepts. See *id.*

The executive branch's promise to the judiciary was broken even before it was made. The DEA's 'Special Operations Division' ('SOD') has, since at least 2005,

obtained and disseminated information from intelligence sources (including NSA) and provided that information to law enforcement. *See* Exhibit J – DEA and NSA Team Up to Share Intellgience, Leading to Secret Use of Surviellance in Ordinary Investigations, Electronic Frontier Foundation, August 6, 2013.[15] The fact that the government has been recording the call data and spying on the internet activity of every American, and then providing this information to ordinary domestic law enforcement, is particularly frightening in light of the fact that federal law enforcement has a rather lengthy and inglorious history of using its intelligence and law enforcement powers to subvert civil rights organizations and suppress political dissent.[16]

Perhaps even more disturbing than this Orwellian surveillance is the fact that the executive branch has taken extraordinary and dishonest measures to conceal it from judicial scrutiny. Law enforcement agents working with SOD have been instructed to conceal the source of the information and come up with a new 'clean' source for the information. *See* Exhibit J. The IRS manual's section on SOD, for example, stated that:

> "Usable information regarding these leads must be developed from such independent sources as investigative files, subscriber and toll requests, physical surveillance, wire intercepts, and confidential source information. **Information obtained from SOD in response to a search or query request cannot be used directly in any investigation (i.e. cannot be used in affidavits, court proceedings, or maintained in investigative filed.**"

See Exhibit K – Exclusive: IRS manual detailed DEA's use of hidden intel evidence, Reuters, Aug. 7, 2013.[17] Similarly, government instructional manuals for the Hemisphere Project, which were released by the New York Times, instruct the agents using data from the program to lie about how the data was acquired: "All requestors are instructed to never refer to Hemisphere in any official document. If there is no alternative

---

[15] https://www.eff.org/deeplinks/2013/08/dea-and-nsa-team-intelligence-laundering

[16] *See* Seth Rosenfeld, Subversives: The FBI's War on Student Radicals, and Reagan's Rise to Power (2012).

[17] Available at: http://www.reuters.com/article/2013/08/07/us-dea-irs-idUSBRE9761AZ20130807.

to referencing a Hemisphere request, then the results should be referenced as information obtained from an AT&T subpoena." *See* Exhibit L – Hemisphere Project Slide Deck, N.Y. Times.[18]

The use of what the government calls "parallel construction"[19] is designed to prevent the Courts from scrutinizing the government's surveillance and information-sharing practices by attempting to prevent the information from being disclosed to defense counsel, the courts, *and even prosecuting attorneys*, according to documents provided to Reuters. See Exhibit M - Exclusive: U.S. directs agents to cover up program used to investigate Americans, Reuters, August 5, 2013.[20] Because prosecutors are kept in the dark about the use of this information, they can 'honestly' deny to the court that the information has been used, thus circumventing the ethical responsibilities imposed on prosecutors by *Brady* and the due process clause of the constitution to provide defense counsel with information which may lead to suppression of evidence.

Because law enforcement's policy has been to withhold the use of SOD or similar information from prosecuting attorneys (a theme which was also repeated with the use of Stingray technology, described below), a denial from the U.S. Attorney that NSA, SOD, Hemisphere or similar intelligence source provided information for an investigation is simply not credible. Defendants therefore request the Court enter an order, directed at the NSA, DEA SOD, Hemisphere, and U.S. Department of Justice to disclose all communications between intelligence services and law enforcement related to this case. In addition, defendants ask the Court to compel the government to disclose the sources of the call record details for the hundreds of thousands of phone calls on which the government's wiretap investigation was primarily based and for which they have

---

Available at: http://www.nytimes.com/interactive/2013/09/02/us/hemisphere-project.html?_r=0

Retired Federal District Court Judge and Harvard Law School professor Nancy Gertner has more honestly described this practice as "phonying up investigations."

Available at: http://www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805?irpc=932

disclosed no legitimate source of information. Finally, defense counsel requests an order for disclosure of *all* phone numbers, call records (with phone numbers for each call), and cell-site data obtained in the investigation. Without information on the methods the government used to seize the call detail records, defendants will not be afforded a fair opportunity to challenge the lawfulness of the inclusion of this data in the government's wiretap applications.

F. The government must disclose all use of Stingrays against the defendants

Before there was Edward Snowden, there was Daniel Rigmaiden. Mr. Rigmaiden, the defendant in Arizona District Court Case No. 08-cr-814-DGC, was charged with a series of fraud and identity theft offenses after federal agents located and arrested him in the Bay Area using a device called a "stingray." See *United States v. Rigmaiden*, 2013 U.S. Dist. LEXIS 65633. (D.Ariz. 2013). A "stingray," also known as a triggerfish, ISMI catcher, WIT technology, or by several other titles, is a mechanical device which intercepts the signal of a cellular telephone by mimicking a cell phone tower. All cell phones must communicate constantly with cellular towers in order to function, and a Stingray works by intercepting those signals and obtaining all of the information transmitted from the device to the tower. By intercepting these signals, the stingray operator is able to locate the precise location of a specific telephone number, obtain the phone number for a specific telephone if the location is known, track incoming and outgoing calls and text messages, and even listen to or record conversations. In short, a stingray is a device which can act like a GPS tracker, pen register, wiretap, and phone number identifier – all in one briefcase-sized package. *See* Exhibit N – How 'Stingray' devices work, Wall Street Journal, September 21, 2011.[21]

The government did not come out and acknowledge their use of a Stingray in the Rigmaiden case, and instead went to great lengths to conceal it. A warrant affidavit submitted to then-Magistrate Judge Seeborg in the case made no mention of the use of a

[21] Available at: http://blogs.wsj.com/digits/2011/09/21/how-stingray-devices-work/

stingray, and rather misleadingly stated that the agents sought authorization for the assistance of Verizon wireless to use a 'mobile tracking device.' After the case was filed, the government did not formally acknowledge the use of the stingray until nearly three years of discovery litigation – referring instead to information obtained from a "source of information" which was actually a machine. *See id.*, at *60 – 63.

In the wake of the revelation that the government had in fact used the stingray, there was some communication between the magistrate judges in the Northern District of California and the U.S. Attorney's office related to the use of these devices. These communications are evidenced by emails obtained and published by the ACLU by former U.S. Attorney Criminal Division Chief Miranda Kane (Exhibit O – N.D. California U.S. Attorney Emails). In a May 23, 2011 email to all criminal AUSAs in the Northern District, Ms. Kane stated that:

> "As some of you may be aware, our office has been working closely with the magistrate judges in an effort to address their collective concerns regarding whether a pen register is sufficient to authorize the use of law enforcement's WIT technology (a box that simulates a cell tower and can be placed inside a van to help pinpoint an individual's location with some specificity) to locate an individual. **It has recently come to my attention that many agents are still using WIT technology in the field although the pen register application does not make that explicit**."

Exhibit O.

Her email goes on to request information from all U.S. Attorneys who have requested pen registers since January 2011 on whether WIT technology was used, and to add a layer of review until "we have an opportunity to discuss the issue with the bench and revise the language in our common application." Exhibit O. A follow up email from Karen Beausey of the U.S. Attorney's office states that agents may have decided to use stingrays after obtaining a pen register order and "may or may not have told you about this decision." *id.* Based on these emails, it appears that law enforcement agents may have once again failed to inform (if not deliberately misled) federal prosecutors regarding the electronic surveillance they conducted as part of their investigations.

A number of facts about this case make it particularly likely that stingrays were used to locate defendants, identify their telephones, or keep track of their phone calls. The first is the initial discovery of Mr. Cabrera-Arteaga's phone, which is referred to in the application as coming from a "Source of Information" which is not described at all in the GPS warrant, and is contrasted with "Confidential Source 1" who is described shortly thereafter. See Exhibit P – GPS Warrant Application, at Bates 7000011. Second, the government's statements in the pen register applications have major inconsistencies as to the source of the phone numbers they are able to identify. And most of all, the government repeatedly obtains new cell phone numbers from undisclosed "sources of information" who appear and provide cell phone numbers to government agents just as a suspect changes his or her phone number, then disappear from the case narrative with little or no disclosure of their identity or reason for providing this information. *See*, e.g. Exhibit Q – Pen Register Application Excerpts, at Bates 1001172, 1001225, 1001350.

Because there is reason to believe that stingrays were used in this case, and their use is at best constitutionally problematic, the defense requests the following information be turned over: all communications responsive to Miranda Kane's request for information regarding the use of stingray technology in the Northern District, the identity of every 'source of information' who allegedly provided a cell phone number for a defendant in the case, a full disclosure from the U.S. Attorney and federal law enforcement regarding the use of stingrays in this case, and an evidentiary hearing at which defense counsel can call the government agents for questioning on the use of stingray technology in the case.

Respectfully Submitted,

DATED: October 2, 2013

/s/ Jeffry Glenn
JEFFRY GLENN
Attorney for Mr. Lara