UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER PURSUANT TO 18 U.S.C. §§ 2703(c) AND 2703(d) DIRECTING AT&T, SPRINT/NEXTEL, T-MOBILE, METRO PCS AND VERIZON WIRELESS TO DISCLOSE CELL TOWER LOG INFORMATION	M-50

JAMES C. FRANCIS IV
UNITED STATES MAGISTRATE JUDGE

The United States of America (the "Government") seeks an order pursuant to the Stored Communications Act ("SCA") requiring various cellular telephone service providers to disclose historical cell site data from cell towers located near a specified New York City address for a particular four-and-one-half hour time period. I asked that the Government provide me with a memorandum supporting its position that the requested information was obtainable, and further invited the New York Civil Liberties Union and American Civil Liberties Union (collectively, the "ACLU") to submit their views on the question as amici curiae.[1]

Information Sought

The Government explains that there are two ways to obtain historical cell site data. In the typical case, the Government requests information connected to a particular cell phone number and (if the application is granted) retrieves "a list of all calls to and from the telephone number, along with the locations and

[1] I am grateful to the ACLU for its thorough and helpful submission, which was of considerable assistance in resolving the Government's application. The ACLU's work is especially impressive, given that counsel were unable to review the actual application at issue, which is not publicly available.

sectors (or 'faces') of the cell towers through which each call originated and terminated," thus providing information helpful in determining the "approximate locations of cellular telephones during the sending and receipt of calls." (Letter of Jason A. Masimore dated May 7, 2014 ("Masimore 5/7/14 Letter") at 1-2).

This application, on the other hand, centers not on a particular cell phone number, but on the cell towers in the area of an identified location. The information sought "consists of a list for a particular cell tower from the specified date and time period of the subscribers' cellular telephone numbers connecting to that tower, along with the times of the calls and the digits dialed or the call numbers of the telephones calling into the subscribers' cellular telephones connecting through the tower," information that can help establish "that the listed cellular telephones were somewhere in the vicinity of that particular cell tower during that time period." (Masimore 5/7/14 Letter at 2). The information gathered here -- specifically, the telephone numbers that connected to the cell towers during the pertinent time period -- will be compared to similar information gathered from other locations relevant to the investigation to determine numbers that were used at multiple locations, as well as numbers that match those that law enforcement has learned are associated with certain persons under investigation for the series of crimes at issue.

Discussion

A. Authorization under the Stored Communications Act

The SCA permits the Government to obtain an order requiring "a

provider of electronic communication service . . . to disclose a record or other information pertaining to a subscriber or customer of such service (not including the contents of communications)" when the Government offers "specific and articulable facts showing that there are reasonable grounds to believe that the . . . records . . . sought[] are relevant and material to an ongoing criminal investigation." 18 U.S.C. §§ 2703(c)(1), (d).

The ACLU argues that a cell tower dump is not authorized under the statute because "Congress phrased the disclosure provision of § 2703(c) in the singular: 'a subscriber or customer of such service.'" (Letter of Nathan Freed Wessler, et al. dated May 20, 2014 ("Wessler 5/20/14 Letter"), at 7). Although this argument has some intuitive appeal, it is easily refuted: "[i]n determining the meaning of any Act of Congress, unless the context indicates otherwise[,] words importing the singular include and apply to several persons, parties, or things." 1 U.S.C. § 1. The ACLU argues that the "use of the singular article . . . is part of Congress's comprehensive scheme to strictly limit permissible government intrusions into the privacy of cell phone users." (Wessler 5/20/14 Letter at 8). However, this generalized "context" is insufficient to overrule "the default rule of statutory construction that words importing the singular include the plural meaning." Carrow v. Merit Systems Protection Board, 564 F.3d 1359, 1366 (Fed. Cir. 2009) (examining legislative history for indication that statutory term "an Executive agency" was intended to preclude

plural meaning).[2]

The ACLU further contends that even if the SCA as a whole does not prohibit cell tower dumps, they can never be obtained under § 2703(d): the Government "cannot possibly meet th[e] [statute's] standard because it seeks vast quantities of irrelevant and immaterial -- yet extraordinarily sensitive -- information about hundreds or thousands of wholly innocent parties." (Wessler 5/20/14 Letter at 8). Noting that courts have described § 2703(d)'s standard as akin to "reasonable suspicion," In re Application of the United States of America for Historical Cell Site Data, 724 F.3d 600, 616 (5th Cir. 2013) (Dennis, J. dissenting) (hereinafter In re Fifth Circuit Application) (denominating the standard "reasonable suspicion"); In re Application of the United States of America for an Order Pursuant to 18 U.S.C. § 2703(d), 707 F.3d 283, 287 (4th Cir. 2013) ("This is essentially a reasonable suspicion standard."), the ACLU cites

[2] The ACLU also contends that the view "that the government may obtain an order under § 2703(c) about a subscriber of service A from service B" ignores the statutory text authorizing disclosure of a record "'pertaining to a subscriber or customer of such service.'" (Wessler 5/20/14 Letter at 8 (quoting 18 U.S.C. 2703(c))). Under the order sought, the only information that service A could provide about a service B subscriber is that subscriber's phone number, either because a service A subscriber dialed it or because a service B subscriber dialed a service A phone number. This is the same information available from a conventional pen register, which captures outgoing "dialing, routing, addressing, or signaling information" from a cell phone or other electronic or wire communication device, or a trap and trace device, which captures "incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication." 18 U.S.C. § 3127(a)(3)-(4).

cases regarding so-called Terry stops to support its argument that "the 'reasonable suspicion' standard requires an evaluation of the facts pertinent to the individual being searched or seized." (Wessler 5/20/14 Letter at 9 (citing Ybarra v. Illinois, 444 U.S. 85, 94 (1979)).

While clever, this argument ignores the actual language of the statute, which does not use the phrase "reasonable suspicion," but requires only "specific and articulable facts showing that there are reasonable grounds to believe that the . . . records . . . sought[] are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). Thus there is no indication in the text (or in the legislative history) that Congress intended to import the standards guiding Terry stops into the SCA. Nor is it likely that the courts using this shorthand intended to graft onto the statutory language the doctrine arising out of the limited investigation stop cases. A better interpretation is that, when used in connection with the SCA, the phrase merely indicates that the standard "is a lesser one than probable cause." In re Application of the United States of America for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government, 620 F.3d 304, 313 (3d Cir. 2010) (hereinafter In re Third Circuit Application).

Accordingly, the type of order sought here is authorized by the statute.

B. The Warrant Requirement

The Fourth Amendment can, of course, trump statutory

authorization either by requiring the Government to show probable cause to obtain the information sought here or, perhaps, by prohibiting such searches altogether. That amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const., amend. IV. It requires law enforcement to obtain a warrant before executing a search, thus "interpos[ing] a magistrate between the citizen and the police . . . to ensure that an objective mind might weigh the need to invade that privacy in order to enforce the law." United States v. Voustianiouk, 685 F.3d 206, 211 (2d Cir. 2012) (internal quotation marks omitted). Justice Harlan's concurrence in Katz v. United States, 389 U.S. 347 (1967), a touchstone of Fourth Amendment jurisprudence, formulated a "twofold requirement" for determining whether government action constitutes a search: "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" Id. at 361 (Harlan, J. concurring); see also United States v. Jones, __ U.S. __, __, 132 S. Ct. 945, 950 (2012) ("Our [] cases have applied the analysis of Justice Harlan's concurrence in [Katz], which said that a violation occurs when government officers violate a person's 'reasonable expectation of privacy.'" (quoting Katz, 389 U.S. at 360 (Harlan, J. concurring)). The ACLU argues that there is a reasonable expectation of privacy in cell

tower records from which individuals' location can be determined.[3] (Wessler 5/20/14 Letter at 13).

1. "Dragnet Type" Surveillance

In United States v. Knotts, 460 U.S. 276 (1983), the Supreme Court approved the warrantless use of a beeper to track a vehicle's movements on public roads. Id. at 281-82. Noting the respondent's fear that the holding could usher in "'twenty-four hour surveillance of any citizen of this country . . . without judicial knowledge or supervision,'" the Court observed that, "if such dragnet type law enforcement practices . . . should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable." Id. at 283-84. The ACLU contends that cell tower dumps violate reasonable expectations of privacy "because they involve just th[is] sort of

[3] The Government asserts that the records it seeks will enable it to determine "that the listed cellular telephones were somewhere in the vicinity of that particular cell tower during that time period" (Masimore 5/7/14 Letter at 2), and it appears that the information will allow the Government only to determine whether a particular subscriber's cell phone is in proximity to the subject cell tower and to identify the sector of the tower to which the cell phone connected. The Government indicates that it will not be using additional tools to further pinpoint location. (Letter of Jason A. Masimore dated May 23, 2014, at 2 n.1); see In re Smartphone Geolocation Data Application, __ F. Supp. 2d __, __, 2013 WL 5583711, at *7 (E.D.N.Y. 2013) ("Cell-site location is arguably the least precise of the three methods currently used, though that precision can be substantially enhanced through triangulation of signals from multiple towers."); In re Application of the United States of America for an Order Pursuant to 18 U.S.C. § 2703(d) Directing Providers to Provide Historical Cell Site Locations Records, 930 F. Supp 2d 698, 701 (S.D. Tex. 2012) (hereinafter In re S.D. Tex. Application) ("[R]efinements in location technology regarding cell site information" actually "enables [the Government] to plot with great precision where the cell phone user has been during a given time period.").

'dragnet type' surveillance of hundreds or thousands of innocent people." (Wessler 5/20/14 Letter at 13).

I cannot agree that the Government's application here raises the spectre of "wholesale surveillance" suggested in Knotts and some of the cases following it. Such concerns center on the possibility of the Government tracking an individual's (or a number of individuals') every movement over a period of time. See Knotts, 460 U.S. at 284 (mentioning "twenty-four hour surveillance of any citizen of this country"); United States v. Katzin, 732 F.3d 187, 191-92, 205 (3d Cir. 2013) (holding warrantless GPS tracking of vehicle for several days generating "highly accurate record of the tracker's whereabouts throughout its period of operation" unjustified), vacated on grant of reh'g en banc, 2013 WL 7033666 (3d Cir. Dec. 12, 2013); United States v. Pineda-Moreno, 617 F.3d 1120, 1125-26 (9th Cir. 2010) (Kozinski, C.J., dissenting from denial of rehearing en banc) (equating GPS tracking device that continuously recorded car's location with "dragnet-type law enforcement practices" of Knotts and worrying that "[b]y tracking and recording the movements of millions of individuals the government can use computers to detect patterns and develop suspicions"); United States v. Marquez, 605 F.3d 604, 610 (8th Cir. 2010) ("It is imaginable that a police unit could undertake 'wholesale surveillance' by attaching [electronic tracking] devices to thousands of random cars and then analyzing the volumes of data produced for suspicious patterns of activity."); United States v. Garcia, 474 F.3d 994, 998 (7th Cir. 2007) ("The new technologies

enable, as the old (because of expense) do not, wholesale surveillance. One can imagine the police affixing GPS tracking devices to thousands of cars at random, recovering the devices, and using digital search techniques to identify suspicious driving patterns."). That is not at issue here. Rather, the Government seeks to retrieve phone numbers used during a particular time period in a particular area to be cross-referenced with data generated from other areas relevant to the investigation during other relevant time periods.[4] There is no possibility that widespread tracking of the locations of individuals could ensue if the application is granted. See In re Application of the United States of America for an Order Authorizing the Release of Historical Cell-Site Information, 809 F. Supp. 2d 113, 122, 126-27 (E.D.N.Y. 2011) (hereinafter In re E.D.N.Y. Application) (holding that "cumulative cell-site-location records" require a warrant because of the significant "governmental intrusion into information which is objectively recognized as highly private" -- that is, the Government's "surveillance of [one's] movements over a considerable time period"); cf. Commonwealth v. Augustine, 467 Mass. 230, 251-55, 4 N.E.3d 846 (2014) ("[T]he tracking of the defendant's

[4] The ACLU supposes an extremely broad search, which it characterizes as a "fishing expedition." (Wessler 5/20/14 Letter at 14). However, as explained above, the order sought is more like what the ACLU calls a "typical tower dump" intended to cross-reference numbers acquired with numbers that the Government has determined to be relevant in its investigation. (Wessler 5/20/14 Letter at 14). The ACLU recognizes that this type of request does not raise the "especially acute constitutional concerns" that would have been implicated by its more expansive hypothetical search. (Wessler 5/20/14 Letter at 14).

movements . . . for two weeks was more than sufficient to intrude upon the defendant's expectation of privacy safeguarded [by the Massachusetts Constitution].").

2. The Voluntary Disclosure Doctrine

In United States v. Miller, 425 U.S. 435 (1976), the petitioner sought to suppress certain documents connected with his bank accounts, which had been obtained without a warrant. Id. at 437-38. The Supreme Court held that the documents did not fall "within a protected zone of privacy," and therefore the Fourth Amendment was not implicated in law enforcement's acquisition of them. Id. at 440. It noted that the information contained in the records, which included checks, financial statements, and deposit slips, was "voluntarily conveyed to the banks." Id. at 442.

> The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.

Id. at 443 (internal citations omitted).

Three years later, in Smith v. Maryland, 442 U.S. 735 (1979) the Court applied the reasoning of Miller and the cases on which it relied to "the question whether the installation and use of a pen register constitutes a 'search' within the meaning of the Fourth Amendment." Id. at 736 (footnote omitted). It held that the petitioner had no "legitimate expectation of privacy regarding the numbers he dialed on his phone" because "[t]elephone users . . .

typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes." Id. at 742-43. This was true even though the defendant had "'us[ed] the telephone in his house to the exclusion of all others,'" because "[a]lthough [his] conduct may have been calculated to keep the contents of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed." Id. (first alteration in original) (emphasis omitted). Smith thus reaffirmed what the Court has consistently held: "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." Id. at 743-44. Smith and Miller remain the "prevailing case law." United States v. Pascual, 502 F. App'x 75, 80 & n.6 (2d Cir. 2012).

Many courts have held that this voluntary disclosure doctrine (also known as the "third-party disclosure doctrine") compels the conclusion that the Government's acquisition of cell site location data is not a "search" within the meaning of the Fourth Amendment. See, e.g., United States v. Caraballo, 963 F. Supp. 2d 341, 359-60 (D. Vt. 2013) ("Smith and Miller thus support a conclusion that a cell phone user generally has no reasonable expectation of privacy in cell site information communicated for the purpose of making and receiving calls in the ordinary course of the provision of cellular phone service."); In re Smartphone Geolocation Data Application, __ F. Supp. 2d at __, 2013 WL 5583711, at *14 ("Under existing law []

a user does not have a reasonable expectation of privacy as to geolocation data."); United States v. Madison, No. 11-60285-CR, 2012 WL 3095357, at *9 (S.D. Fla. July 30, 2012) ("[T]he third-party disclosure doctrine relied upon by Smith requires the finding that society is not prepared to recognize as legitimate any subjective expectation that Defendant might have had in the cell-tower location data for his cell-phone usage."); United States v. Graham, 846 F. Supp. 2d 384, 389, 400 (D. Md. 2012) ("Based on clear Supreme Court . . . precedent, this Court finds the third-party doctrine applicable to historical cell site location information."). These courts have noted that "[a]s part of the ordinary course of business, cellular phone companies collect information that identifies the cell towers through which a person's calls are routed." Graham, 846 F. Supp. 2d at 400. Contrary to the ACLU's contention (Wessler 5/20/14 Letter at 17), this is information that cell phone users voluntarily disclose -- "[a]fter all, if the phone company could not locate a particular cell phone, there would be no means to route a call to that device, and the phone simply would not work." In re Smartphone Geolocation Data Application, __ F. Supp. 2d at __, 2013 WL 5583711, at *14; see also Madison, 2012 WL 3095357, at *8 ("All cell users are aware that cell telephones do not work when they are outside the range of the communication company's cell-tower network. . . . Thus, . . . cell-phone users have knowledge that when they place or receive calls, they, through their cell phones, are transmitting signals to the nearest cell tower, and, thus, to their communications service

providers."). And it is "common knowledge that communications companies regularly collect and maintain all types of non-content information regarding cell-phone communications, including cell-site tower data, for cell phones for which they provide service." Madison, 2012 WL 3095357, at *8; see also In re Fifth Circuit Application, 724 F.3d at 611-12, 613-14 (noting that "[t]he cell service provider collects and stores historical cell site data for its own business purposes, perhaps to monitor or optimize service on its network or to accurately bill its customers" and that users voluntarily convey information about their location when they place a call, even if they do not "directly inform [the] service provider of the location of the nearest cell phone tower"); In re Smartphone Geolocation Data Application, __ F. Supp. 2d at __, 2013 WL 5583711, at *7-10 (discussing widespread public knowledge of ability and practice of cell phone service providers to track customers' locations); In re E.D.N.Y. Application, 809 F. Supp. 2d at 121 (calling it a "doubtful proposition" that cell phone users are unaware that location data is collected and stored by service providers). But see In re Third Circuit Application, 620 F.3d at 317 ("[I]t is unlikely that cell phone customers are aware that their cell phone providers collect and store historical location information."). I agree that Smith and Miller dictate the outcome here, where the subscribers are aware that use of their cell phones necessitates disclosure of the information sought.

The ACLU cites United States v. Warshak, 631 F.3d 266 (6th Cir. 2010) for the proposition that "the fact that cell phone

location information is handled by a third party is not dispositive." (Wessler 5/20/14 Letter at 18). But Warshak dealt with the disclosure of the contents of a defendant's e-mails. Warshak, 631 F.3d at 283. And the Court in Smith noted an exception to the voluntary disclosure doctrine for the content of communications that are routed through a third party. Smith, 442 U.S. at 741; see also Madison, 2012 WL 3095357, at *9 n.11 (noting "content exception to the third-party-disclosure doctrine as it relates to communications providers"); In re E.D.N.Y. Application, 809 F. Supp. 2d at 122-25 (discussing "content exception [] incorporated, by dicta, into Fourth Amendment telephonic communications case law in Smith"). Warshak is therefore inapposite here, where the Government does not seek the contents of communications.

3. Constitutionally Protected Spaces

To be sure, much of the information the Government seeks will have been generated by people using their cell phones in their own homes. The ACLU argues that the cell tower dump therefore constitutes a Fourth Amendment search of "constitutionally protected spaces." (Wessler 5/20/14 Letter at 14-15).

The Supreme Court has "not deviated from th[e] basic Fourth Amendment principle" that "[s]earches and seizures inside a home without a warrant are presumptively unreasonable." United States v. Karo, 468 U.S. 705, 714-15 (1984). Accordingly, the Court held in Karo that law enforcement monitoring of a beeper on a can of ether while the can was in a private residence was a Fourth

Amendment search requiring a warrant because it revealed "critical fact[s] about the interior of the premises" that the Government could not have obtained through visual surveillance. Id. at 715. Similarly, in Kyllo v. United States, 533 U.S. 27 (2001), the warrantless use of a "thermal-imaging device aimed at a private home from a public street" was held to be unconstitutional because "obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical intrusion into a constitutionally protected area constitutes a search." Id. at 29, 34 (citation omitted) (internal quotation marks omitted). Thus, it is certainly correct that the Supreme Court has repeatedly recognized that government intrusion into the home without a warrant intrudes on a reasonable expectation of privacy.

Nonetheless, Karo and Kyllo do not alter the analysis here. As Smith makes clear, the voluntary disclosure doctrine applies even where the disclosures are made from the protected space of the home. Smith, 442 U.S. at 743 ("But the site of the call is immaterial for the purposes of analysis in this case. . . . The fact that he dialed the number on his home phone rather than on some other phone could make no conceivable difference . . . ."); see also In re Smartphone Geolocation Data Application, __ F. Supp. 2d at __, 2013 WL 5583711, at *12-13 (finding location of origination of communication "not . . . useful" in deciding whether to issue authorization for cell site data and therefore applying voluntary disclosure doctrine); Caraballo, 963 F. Supp. 2d at 356

(stating, in case regarding Government "pinging" target cell phone, that "[a] Fourth Amendment analysis entirely dependent upon the fortuity of a criminal defendant entering his or her own home during the pinging process is likely to prove [] unworkable . . . ."). But see In re Application of the United States of America for Historical Cell Site Data, 747 F. Supp. 2d 827, 835-37 (S.D. Tex. 2010) (denying request for historical cell site data based, in part, on location of phone in non-public places), vacated by In re Fifth Circuit Application, 724 F.3d at 615.

4. Discretion

Finally, the ACLU argues that, even if the SCA and the Constitution permit issuance of the requested order on a less stringent showing than probable cause, it is within my discretion to require that the Government meet the higher standard. (Wessler 5/20/14 Letter at 10-12). I agree that a judge has such discretion.

The operative statutory language states that "a court order for disclosure . . . may be issued by any court that is a court of competent jurisdiction and shall issue only if" the standard is met. 18 U.S.C. § 2703(d). The Third Circuit has observed that the phrase "may be issued" is "the language of permission, rather than mandate." In re Third Circuit Application, 620 F.3d at 315. Additionally, the direction that an order "shall issue only if" the standard is met "describe[s] a necessary condition, not a sufficient condition." Id. at 316 (internal quotation marks omitted). But see In re Fifth Circuit Application, 724 F.3d at

606-08 (rejecting Third Circuit's interpretation). If Congress meant otherwise, it could have excised the word "only" from the statute; however, "the statute does contain the word 'only' and neither [I] nor the Government is free to rewrite it." In re Third Circuit Application, 620 F.3d at 315.

Under the voluntary disclosure doctrine, an individual's privacy interest in shared information is attenuated but not necessarily eviscerated altogether. See, e.g., Smith, 442 U.S. 741 (voluntary disclosure doctrine does not extend to contents of communications). Certain searches by the Government of information that is voluntarily but selectively disclosed may be so invasive that it would be prudent to require a showing of probable cause. With emerging and as-yet-unknown technologies, such searches are likely to become easier, cheaper, and more prevalent; it may, then, be time to scrutinize the voluntary disclosure doctrine more closely. See Jones, __ U.S. at __, 132 S. Ct. at 957 (Sotomayor, J. concurring) ("More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.").

Nevertheless, I will not require a warrant here because the information voluntarily disclosed -- the telephone numbers associated with communications in a general location -- does not implicate privacy interests to the same degree as, for example, the content of those communications. I will, however, require the Government to submit an amended application that (1) provides more

specific justification for the time period for which the records will be gathered and (2) outlines a protocol to address how the Government will handle the private information of innocent third-parties whose data is retrieved. See In re S.D. Tex. Application, 930 F. Supp. 2d at 702 ("[I]n order to receive such data, the Government at a minimum should have a protocol to address how to handle this sensitive private information."); see also In the Matters of the Search of Cellular Telephone Towers, 945 F. Supp 2d 769, 771 (S.D. Tex. 2013) (issuing warrant for cell tower records but requiring, among other things, that "any and all original records and copies . . . determined not to be relevant to the . . . investigation" be returned to cell service providers).

Conclusion

The Government is directed to submit, within seven days of the date of this order, an amended application that (1) re-evaluates and justifies the time period for which the cell tower records are requested and (2) provides a plan to address the protection of private information of innocent third-parties whose data is disclosed to the Government. If that information satisfies me that the privacy rights of subscribers are adequately protected, the requested order will issue.

SO ORDERED.

James C. Francis IV

JAMES C. FRANCIS IV
UNITED STATES MAGISTRATE JUDGE

Dated: New York, New York
May 30, 2014

Copies mailed this date:

Jason A. Masimore, Esq.
Assistant U.S. Attorney
One St. Andrew's Plaza
New York, NY 10007

Nathan Freed Wessler, Esq.
Brett Max Kaufman, Esq.
Alex Abdo, Esq.
Ben Wizner, Esq.
Catherine Crump, Esq.
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004

Christopher T. Dunn, Esq.
Arthur N. Eisenberg, Esq.
New York Civil Liberties Union Foundation
125 Broad Street, 19th Floor
New York, NY 10004