LEGAL DEPARTMENT

AMERICAN CIVIL LIBERTIES UNION FOUNDATION

NATIONAL OFFICE
125 BROAD STREET,
18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500
F/212.549.2651
WWW.ACLU.ORG

OFFICERS AND DIRECTORS
*SUSAN N. HERMAN*
*PRESIDENT*

ANTHONY D. ROMERO
*EXECUTIVE DIRECTOR*

May 20, 2014

**By Email**

The Honorable James C. Francis IV
United States Magistrate Judge
United States District Court for the Southern District of New York
Daniel Patrick Moynihan U.S. Courthouse
500 Pearl Street
New York, NY 10007

**ACLU Response to Government Application for Historical Cell Site Data from Cell Towers in the Vicinity of One Location During a Four-and-One-Half-Hour Time Period**

Dear Judge Francis:

At the Court's invitation, the New York Civil Liberties Union and American Civil Liberties Union (collectively, "ACLU") offer briefing in response to the government's May 7, 2014, letter-brief ("Gov't Ltr.-Br."), in which the government seeks an order under 18 U.S.C. § 2703(d) for historical cell site location records from a number of cell towers near a New York City address. The ACLU appreciates the opportunity to share its views on this matter and welcomes additional queries from the Court. Should this Court decide to hold a hearing on the government's application, the ACLU would be pleased to participate in oral argument.[1]

The ACLU understands that this letter-brief is longer than would normally be submitted to the Court, but there is good reason for the length. To our knowledge, this is the first public brief explaining the constitutional and

1 The ACLU has been involved as direct counsel or amici in numerous cases involving electronic location tracking, and believes its expertise can be of aid to the Court here. *See, e.g.*, *United States v. Jones*, 132 S. Ct. 945 (2012) (GPS tracking); *People v. Weaver*, 909 N.E.2d 1195 (N.Y. 2009) (GPS tracking); *United States v. Quartavious Davis*, No. 12-12928-EE (11th Cir. argued Apr. 25, 2014) (request to cell service provider for defendant's historical cell site location information); *United States v. Skinner*, 690 F.3d 772 (6th Cir. 2012) (real-time cell phone location tracking); *United States v. Rigmaiden*, No. CR 08–814–PHX–DGC, 2013 WL 1932800 (D. Ariz. May 8, 2013) (tracking using cell site simulator device).

statutory concerns with a "cell tower dump" like that sought by the government here. Moreover, other than three short opinions by a single magistrate judge in Texas,[2] there is no caselaw on tower dumps from any court that could be cited as a shortcut to full argumentation. Finally, the length of this brief is also a result of the sealing of the government's application filed pursuant to 18 U.S.C. § 2703(d). Because the ACLU has virtually no information about the factual predicate for the government's application, it cannot effectively tailor this brief to the details of the case. This letter-brief endeavors to set out the full range of arguments potentially responsive to the government's claims.[3] Additionally, the government's letter-brief mainly addresses the third party doctrine, Gov't Ltr.-Br. at 3–7, leaving the ACLU to present and explain every other legal issue bearing on the legality of tower dumps.

## INTRODUCTION

The government seeks an order under 18 U.S.C. § 2703(d) for what is known as a "cell tower dump"—a set of records revealing every cell phone that connected with a set of cell towers over a specified period of time. An order compelling cell service providers to comply with this request would implicate the privacy of hundreds or thousands of non-suspects who made or received calls or data connections in the vicinity of the targeted towers during the specified times. Indeed, because cell tower dumps allow the government to learn the locations and movements of large numbers of innocent people, they directly implicate timely and trenchant concerns about mass surveillance. A cell tower dump could be used to identify the people at home in a neighborhood on a particular night, the protestors at a political rally,[4] or the congregants attending services at a mosque, synagogue, or church. Close judicial supervision of tower dump requests is necessary to protect the rights of these innocent parties, and to ensure compliance with the requirements of the Stored Communications Act ("SCA") and the Fourth Amendment.

The SCA imposes a general prohibition on government access to customer records held by cell service providers, subject only to enumerated exceptions. One of those exceptions permits the government to obtain a warrant or court order for records pertaining to "a subscriber to or customer of" the provider. 18 U.S.C. § 2703(c)(1). Because this congressional authorization is

---

2 *See In re Application of the United States for an Order Pursuant to 18 U.S.C. § 2703(d) Directing Providers to Provide Historical Cell Site Locations Records* ("*Owsley Opinion I*"), 930 F. Supp. 2d 698 (S.D. Tex. 2012) (Owsley, M.J.); *In re Search of Cellular Phone Towers* ("*Owsley Opinion II*"), 945 F. Supp. 2d 769, 770 (S.D. Tex. 2013) (Owsley, M.J.); *In re Application of the United States for an Order Pursuant to 18 U.S.C. § 2703(d)* ("*Owsley Opinion III*"), 964 F. Supp. 2d 674 (S.D. Tex. 2013) (Owsley, M.J.).

3 To the extent that knowledge of the underlying facts is necessary to provide adequate adversarial argumentation to the Court, the ACLU respectfully asks that the court unseal the government's application and proposed order with only such narrowly tailored redactions as are necessary to accommodate the government's interest in protecting sensitive details of an ongoing investigation. *See In re Sealing and Non-disclosure of Pen/Trap/2703(d) Orders*, 562 F. Supp. 2d 876, 895 (S.D. Tex. 2008) (Smith, M.J.) ("Legitimate confidentiality interests will almost always be fully accommodated by redacting the troublesome words or passages [rather than sealing the entire file]."). If it will aid the Court's decision, the ACLU respectfully requests the opportunity to provide supplemental briefing after viewing those portions of the application and order that can be unsealed.

4 *See* Andrew E. Kramer, *Russia Defers Aid to Ukraine, and Unrest Persists*, N.Y. Times, Jan. 30, 2014, at A8, *available at* http://www.nytimes.com/2014/01/30/world/europe/ukraine-protests.html (describing Ukrainian government's use of tower dumps to identify protestors at a political protest).

phrased in the singular, there is a serious textual question as to whether the SCA permits tower dumps at all, since they inescapably involve the records of large numbers of people. Tower dumps also raise serious questions concerning the Fourth Amendment, including whether the Constitution permits the bulk surveillance of hundreds or thousands of innocent non-suspects and whether judicial authorizations for tower dumps would constitute the kinds of general warrants long prohibited by our constitutional tradition. The tower dump at issue here appears calculated to enable a true fishing expedition, seeking unspecified information about an apparently unknown suspect from a vast pool of other people's sensitive data.

Even if this Court does not read the SCA or the Fourth Amendment to prohibit the government from seeking tower dump authorizations in all circumstances, it should conclude that tower dumps require the judicial oversight provided by a probable cause warrant. The SCA provides magistrate judges with the discretion to require the government to apply for a warrant pursuant to 18 U.S.C. § 2703(c)(1)(A) instead of an order pursuant to § 2703(c)(1)(B) and § 2703(d). To avoid running afoul of the Supreme Court's skepticism about the constitutionality of "dragnet type" location tracking of large numbers of people, this Court should require the government to proceed via the SCA's warrant mechanism. Recourse to a warrant is also required because the government cannot meet the SCA's reasonable suspicion and relevance standards when it seeks records relating primarily to a group of non-suspects.

Thus, at a minimum, the government must demonstrate probable cause that the tower dump will turn up evidence of a crime, and any warrant issued pursuant to the SCA and Rule 41 must enforce the Fourth Amendment's particularity requirement by minimizing the number of innocent people whose records are sought and by restricting the government's retention and use of any third party records included in the tower dump. A warrant must also require notice to all persons whose location information and other records the government obtains.

## BACKGROUND

As of December 2012, there were more than 326 million wireless subscriber accounts in the United States, responsible for more than two trillion annual minutes of calls and two trillion annual text messages.[5] Cell phone use has become ubiquitous: the number of wireless accounts now exceeds the total population of the United States,[6] 90% of American adults own cell phones,[7] and nearly 40% of U.S. households use only cellular telephones.[8] The cellular network

5 *U.S. Wireless Quick Facts*, CTIA – The Wireless Association, *available at* http://www.ctia.org/advocacy/research/index.cfm/aid/10323.

6 *Id.*

7 Lee Rainie, et al., Pew Research Ctr., *The Web at 25 in the U.S.* 14 (2014), *available at* http://www.pewinternet.org/files/2014/02/PIP_25th-anniversary-of-the-Web_0227141.pdf.

8 Stephen J. Blumberg and Julian V. Luke, Nat'l Ctr. for Health Statistics, *Wireless Substitution: Early Release of Estimates From the National Health Interview Survey, January-June 2013* 2 (2013), *available at* http://www.cdc.gov/nchs/data/nhis/earlyrelease/wireless201312.pdf.

architecture in the United States has grown dramatically to accommodate this wide usage, with more than 300,000 cell towers in use today.[9]

Cellular telephones regularly communicate with their carriers' networks by sending radio signals to these towers, known as "base stations" or "cell sites." *The Electronic Communications Privacy Act (ECPA) (Part II): Geolocation Privacy and Surveillance: Hearing Before the Subcomm. on Crime, Terrorism, Homeland Sec. & Investigations of the H. Comm. on the Judiciary* 113th Cong. 50 (2013) (statement of Matt Blaze, Associate Professor, University of Pennsylvania)[10] ["Blaze Hearing Statement"]. When turned on, "[c]ell phone handsets periodically (and automatically) identify themselves to the nearest base station (that with the strongest radio signal) as they move about the coverage area." *Id.* Phones communicate with the wireless network through these cell sites when a subscriber makes or receives calls or transmits or receives text messages. Smartphones, which are now used by 58% of Americans,[11] typically communicate even more frequently with the carrier's network because they regularly check for new emails, and maintain a persistent Internet connection with the provider of the operating system, such as Google or Apple.[12]

When phones communicate with the network, the service provider automatically logs and retains information about such communications. For example, with respect to phone calls, this information includes the identity of the cell site to which the phone was connected at the beginning and end of each call. Further, most cell sites consist of three directional antennas that divide the cell site into sectors (usually of 120 degrees each),[13] although an increasing number of towers have six sectors.[14] Service providers automatically retain this type of "sector information" too, providing even more precise information about the user's location.[15] Some carriers also calculate and log the user's distance from the cell site.[16]

---

9 *U.S. Wireless Quick Facts*, CTIA, – The Wireless Association, *available at* http://www.ctia.org/advocacy/research/index.cfm/aid/10323.

10 *Available at* http://judiciary.house.gov/hearings/113th/04252013/Blaze%2004252013.pdf.

11 Lee Rainie, et al., Pew Research Ctr., *The Web at 25 in the U.S.* 5 (2014), *available at* http://www.pewinternet.org/files/2014/02/PIP_25th-anniversary-of-the-Web_0227141.pdf.

12 *See A Peek Inside the GTalkService Connection* (June 28, 2010), https://jon.oberheide.org/blog/2010/06/28/a-peek-inside-the-gtalkservice-connection/ ("In short, the GTalkService is a persistent connection maintained from your Android phone to Google's servers at all time. It allows Google to push down messages to your phone in order to perform particular actions.").

13 Thomas A. O'Malley, *Using Historical Cell Site Analysis Evidence in Criminal Trials*, U.S. Attorneys' Bull., Nov. 2011, at 16, 19, *available at* http://www.justice.gov/usao/eousa/foia_reading_room/usab5906.pdf.

14 *See, e.g.*, Exhibit A to Brief of Amici Curiae American Civil Liberties Union Foundation, et al. at 50–57, *United States v. Quartavious Davis*, No. 12-12928-EE (11th Cir. July 17, 2013) (demonstrating that a number of towers in the MetroPCS network in Miami have six sectors).

15 In the sample tower dump records provided by the Government in Exhibit B to its letter brief, this information can be found under the columns labeled "cell face."

16 *See* Verizon Wireless Law Enforcement Resource Team (LERT) Guide 25 (2009), *available at* http://publicintelligence.net/verizon-wireless-law-enforcement-resource-team-lert-guide/ (providing sample records indicating caller's distance from cell site to within .1 of a mile).

The precision of a user's location revealed by the cell site identifier in the carrier's records depends on the size of the sector. The coverage area for a cell site is reduced in areas with greater density of cell towers, with the greatest cell site density (and thus the smallest coverage) in urban areas with large number of smartphone users. Cell site density is increasing rapidly, largely as a result of the growth of internet usage by smartphones—meaning the geolocational information revealed by any given sector is getting more and more accurate.[17]

A request for information regarding all phones that communicated with multiple cell sites over a period of hours, such as the one made in this case, is likely to reveal information about a very large number of phones. Such requests, commonly known as "tower dumps," can—and, in fact, consistently do—involve the collection of hundreds, thousands, or even hundreds of thousands of phone numbers.[18] For example, when the FBI obtained tower dump records for several towers in Arizona in 2010, it received a staggering 150,000 individual users' phone numbers in response.[19] In a 2012 Colorado case, "at least several thousand people's phones" were likely implicated in a series of cell tower dumps requested by local police.[20]

Tower dumps are used by law enforcement agencies "routinely." The Hon. Brian L. Owsley, *The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in Its Electronic Surveillance*, 16 U. Pa. J. Const. L. 1, 17–23 (2013). Cell phone companies reported complying with more than 9,000 cell tower dump requests in 2012.[21] In 2013, Verizon alone performed 3,200 cell tower dumps for law enforcement.[22] AT&T performed 1,034 "cell tower searches."[23] A recent *USA Today* investigation into the practices of 125 police agencies in 33 states revealed that approximately one in four agencies have used a tower dump.[24]

Even given this trend, however, the government's tower dump request in this case is extraordinary for three reasons.

---

17 *See* CTIA – The Wireless Association, Semi-Annual Wireless Industry Survey 2 (2012), *available at* http://files.ctia.org/pdf/CTIA_Survey_MY_2012_Graphics-_final.pdf.

18 Ellen Nakashima, *Agencies Collected Data on Americans' Cellphone Use in Thousands of 'Tower Dumps,'* Wash. Post, Dec. 8, 2013, http://www.washingtonpost.com/world/national-security/agencies-collected-data-on-americans-cellphone-use-in-thousands-of-tower-dumps/2013/12/08/20549190-5e80-11e3-be07-006c776266ed_story.html ("[E]ach [tower dump] request to a phone company yield[ed] hundreds or thousands of phone number of innocent Americans.").

19*Id.*

20 John Kelly, *Cellphone Data Spying: It's Not Just the NSA*, USA Today, Dec.8, 2013, http://www.usatoday.com/story/news/nation/2013/12/08/cellphone-data-spying-nsa-police/3902809/.

21 Nakashima, *supra*.

22 U.S. Data, Verizon Transparency Report (2013), http://transparency.verizon.com/us-data.

23 Location Demands, AT&T Transparency Report (2013), http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport.html.

24 Kelly, *supra.*

First, New York City's high population density means any given tower dump is likely to implicate a tremendous number of people. At more than 27,000 people per square mile, New York City has the highest population density of any major city in the United States.[25] Some Manhattan neighborhood populations are even denser, reaching 96,000 people per square mile.[26] Given this extraordinarily high density, a tower dump targeting even a single tower in New York will likely implicate at least thousands of cell phone users.

Second, New York City has an extremely high concentration of cell sites, meaning the locational data from a single tower dump will be extremely precise. [27] For example, a searcheable database of publicly available information reveals that within a one mile radius of the U.S. District Court for the Southern District of New York at 500 Pearl Street, there are 116 separate towers and 1049 individual antennas.[28] The distance separating many adjoining towers is less than one block. The cell tower density is also high in Upper Manhattan. Within a 2 mile radius of 126th Street and Lenox Avenue, there are 94 towers and 541 antennas.[29] Again, it is not unusual for these towers to be separated by only one or two blocks.

Finally, the request at issue here—for data spanning four hours and thirty minutes[30]—covers an unusually long time frame. Service providers "typically" receive tower dump requests covering 30 minutes or less.[31] When a request for a period longer than one hour is received, service providers may ask police to narrow it, "cognizant that the cell tower dump will contain many mobile device numbers."[32]

These three factors suggest that this Court's evaluation of the government's tower dump request in this case should be especially searching, as the government's request is likely among the broadest requests for such data to date.

---

25 Dep't of City Planning, City of New York, *Population Facts*, NYCPlanning, http://www.nyc.gov/html/dcp/html/census/pop_facts.shtml.

26 Dep't of City Planning, City of New York, *PL-P2 NTA: Population Density by Neighborhood Tabulation Area, New York City, 2010*, http://www.nyc.gov/html/dcp/pdf/census/census2010/m_pl_p2_nta.pdf (showing several neighborhood s in Manhattan with populations of 150 or more people per acre).

27 *See* Blaze Hearing Statement at 9 ("The effect of this trend toward smaller sectors is that knowing the identity of the base station (or sector ID) that handled a call is tantamount to knowing a phone's location. . . [I]n urban areas. . . this area can be quite small indeed, sometimes effectively identifying individuals floors and rooms within buildings").

28 Search conducted using http://www.antennasearch.com.

29 Search conducted using http://www.antennasearch.com using address of 310 Lenox Avenue, New York, NY 10027.

30 Gov't Ltr.-Br. at 1.

31 Letter from William B. Petersen, General Counsel, Verizon Wireless to Sen. Edward J. Markey 4 (Oct. 3, 2013), http://www.markey.senate.gov/documents/2013-12-09_VZ_CarrierResponse.pdf.

32 *Id.*

## ARGUMENT

### I. The Court Should Deny the Government's Request for Tower-Dump Data Under the Stored Communications Act.

#### A. The Stored Communications Act Does Not Permit the Government to Obtain Tower-Dump Data.

The SCA, 18 U.S.C. §§ 2701–12—a subset of the Electronic Communications Privacy Act ("ECPA"), Pub. L. No. 99-508, 100 Stat. 1848 (1986)—comprehensively regulates the disclosure of communications content, records, and other information by electronic communication service providers. As relevant here, the SCA imposes a general prohibition on government access to cell phone location data stored by a cell service provider, subject only to specific statutory exceptions. Although the statute contemplates requests for specific, known users' data, its plain terms do not allow the kind of dragnet search at issue here. *See In re Ames Dep't Stores, Inc.*, 582 F.3d 422, 427 (2d Cir. 2009) ("'Statutory interpretation always begins with the plain language of the statute,' which [the court] consider[s] in 'the specific context in which that language is used, and the broader context of the statute as a whole.'" (citations omitted)); *In re Barnet*, 737 F.3d 238, 246 (2d Cir. 2013) ("'Where the statute's language is plain, the sole function of the courts is to enforce it according to its terms.'").

The SCA provides that an electronic communications service provider "may divulge a record or other information pertaining to *a subscriber to or customer of such service* (not including the contents of communications . . . ) . . . as otherwise authorized in section 2703." 18 U.S.C. § 2702(c)(1) (emphasis added). Section 2703(c) states that "[a] governmental entity may require a provider of electronic communication 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" obtains a warrant, court order, or consent. *Id.* § 2703(c)(1) (emphasis added).

Congress phrased the disclosure provision of § 2703(c) in the singular: "*a* subscriber or customer of such service." On its face, this language permits the government to apply for an order authorizing disclosure of the cell phone location records of a particular suspect. It does not authorize a request for records pertaining to a large set of unidentified persons. As a leading scholar of the SCA has observed, the statute is "silent on court orders that seek records regarding hundreds or even thousands of users." Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. Pa. L. Rev. 373, 402 (2014). Had Congress wanted to authorize bulk requests for multiple customers' or subscribers' data, it could easily have done so, at least as a statutory matter. *See United States v. Hayes*, 555 U.S. 415, 421–22 (2009) (assessing Congress's use of the singular in a statute and explaining that, had Congress meant otherwise, "it likely would have used the plural"). To accept the government's argument is to conclude that Congress intended to authorize broad-based requests for information about thousands of people by using language plainly limited to a single person.

More generally, § 2703(c) reflects Congress's choice in the SCA to protect users' privacy by strictly limiting the circumstances in which the government may obtain cell phone location data. *See* 18 U.S.C. § 2702; S. Rep. No. 99-541, at 3 (1986) (explaining intent to place a check on "technological advances in surveillance devices and techniques" that are available to "overzealous law enforcement agencies," and noting the statute's purpose "to protect privacy interests in personal and proprietary information"). The use of the singular article in § 2703(c) is part of Congress's comprehensive scheme to strictly limit permissible government intrusions into the privacy of cell phone users. *See First Nat'l Bank in St. Louis v. Missouri*, 263 U.S. 640, 657 (1924) (noting the background principle that "'words importing the singular number may extend and be applied to several persons or things,'" but explaining that "obviously this rule is not one to be applied except where it is necessary to carry out the evident intent of the statute").

Further, in this case the government seeks tower-dump data from "various cellular telephone service providers." Gov't Ltr.-Br. at 1. Presumably, the government is trying to identify one or a small number of suspects, whose names, phone numbers, and cell service providers it does not yet know. Assuming, *arguendo*, that the government is seeking information about the location of a single suspect, only a request to *that suspect's* cell service provider would be designed to disclose a record "pertaining to a subscriber or customer of *such* service." The alternative view—that the government may obtain an order under § 2703(c) *about* a subscriber of service A *from* service B—ignores the SCA's plain text. *United States v. Menasche*, 348 U.S. 528, 538–39 (1955) (holding that it is the court's "duty 'to give effect, if possible, to every clause and word of a statute,' rather than to emasculate an entire section, as the Government's interpretation requires" (citation omitted) (quoting *Inhabitants of Montclair Twp. v. Ramsdell*, 107 U.S. 147, 152 (1883)). For good reason, the SCA does not permit this sort of fishing expedition. In the SCA, Congress has carefully constrained government access to cell phone location records to protect individuals' privacy, and it chose not to permit tower dump requests directed at multiple service providers that would expose the records of hundreds or thousands of unidentified non-suspects.

### B. Even if the SCA Does Not Wholly Prohibit Tower Dumps, the Government Cannot Obtain Tower Dump Records Under § 2703(d) Because Those Records Are Not "Relevant and Material" to the Ongoing Criminal Investigation

Even if the threshold language of the SCA does not prohibit applications for tower dumps, this Court should deny the government's request under § 2703(d) because the government cannot satisfy the standard imposed by the statute. To obtain records under that section, the government must meet an "intermediate" standard akin to "reasonable suspicion." But contrary to the government's summary assertion that it meets the statutory standard, Gov't Ltr.-Br. at 9, the government's broad request for tower-dump data in this case cannot possibly meet that standard because it seeks vast quantities of irrelevant and immaterial—yet extraordinarily sensitive—information about hundreds or thousands of wholly innocent parties. The Court should deny the government's request under section 2703(d) and invite it to seek a probable cause warrant under § 2703(c)(1)(A) instead.

The SCA imposes an "intermediate" standard on the government's acquisition of transactional records covered by the statute. *See In re Application of the United States for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government* ("*Third Circuit Opinion*"), 620 F.3d 304, 314–15 (3d Cir. 2010); *accord In re Application of the United States for Historical Cell Site Data* ("*Fifth Circuit Opinion*"), 724 F.3d 600, 619 (5th Cir. 2013). To obtain an order under section 2703(d), the government must "offer[] specific and articulable facts showing that there are reasonable grounds to believe" that "the records or other information sought[] are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). While this standard is lower than the "probable cause" required for criminal warrants, it is more demanding than the mere "relevance" standard governing the issuance of administrative and grand-jury subpoenas. *See Third Circuit Opinion*, 620 F.3d at 314–15; *In re Application of U.S. for an Order for Disclosure of Telecomms. Records & Authorizing the Use of a Pen Register & Trap & Trace*, 405 F. Supp. 2d 435, 449 (S.D.N.Y. 2005) (Gorenstein, M.J.); *In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d 747, 752 (S.D. Tex. 2005) (Smith, M.J.). The imposition of a higher standard for this kind of information was by design: in 1994, Congress raised the existing § 2703(d) standard to "guard against 'fishing expeditions' by law enforcement." S. Rep. No. 103-402, at 31 (1994). As the Fourth Circuit has explained (and as the government itself acknowledges), "[t]his is essentially a reasonable suspicion standard"—the same standard that governs brief physical detentions of individuals under *Terry v. Ohio*, 392 U.S. 1 (1968). *In re U.S. for an Order Pursuant to 18 U.S.C. Section 2703(d)*, 707 F.3d 283, 287 (4th Cir. 2013); Gov't Ltr.-Br. at 2–3; *see United States v. Padilla*, 548 F.3d 179, 187 (2d Cir. 2008) (discussing *Terry* standard).

The Second Circuit has repeatedly explained that the "reasonable suspicion" standard demands "some minimal level of objective justification" supported by "specific and articulable facts[] of unlawful conduct," and that an "inchoate suspicion or mere hunch will not suffice." *United States v. Bayless*, 201 F.3d 116, 132–33 (2d Cir. 2000) (internal quotation marks and citations omitted); *United States v. Glover*, 957 F.2d 1004, 1009–10 (2d Cir. 1992); *see United States v. Sokolow*, 490 U.S. 1, 7 (1989). Crucially, the "reasonable suspicion" standard requires an evaluation of the facts pertinent to the individual being searched or seized. *See Ybarra v. Illinois*, 444 U.S. 85, 94 (1979) ("The 'narrow scope' of the *Terry* exception does not permit a frisk for weapons on less than reasonable belief or suspicion *directed at the person to be frisked*, even though that person happens to be on premises where an authorized . . . search is taking place." (emphasis added)). Thus, several circuits have concluded that presence alone in a suspicious area cannot satisfy "reasonable suspicion," and that "there is no reasonable suspicion merely by association." *United States v. Black*, 707 F.3d 531, 539 (4th Cir. 2013); *see, e.g.*, *id.* at 541 (no reasonable suspicion where defendant was "in a high crime area at night" absent further showing of engagement in criminal activity); *United States v. Lewis*, 674 F.3d 1298, 1313 (11th Cir. 2012) (holding that a court may not "impute an officer's reasonable suspicion of one individual to an associate who is in the vicinity and engaged in purely lawful activity"); *United States v. Cole*, 628 F.2d 897, 899 (5th Cir. 1980) (suppressing evidence obtained via patdown search of individual who arrived at private home as police prepared to execute a search warrant).

Where, as here, the government indiscriminately seeks records implicating the privacy of hundreds or thousands of individuals in one fell swoop, it cannot possibly meet the intermediate "reasonable suspicion" standard. As discussed above, "[a]ny order authorizing a cell tower dump is likely to affect *at least* hundreds of individuals' privacy interests," if not more. *Owsley Opinion II*, 945 F. Supp. 2d at 770 (emphasis added); *see Klayman v. Obama*, 957 F. Supp. 2d 1, 37 n.60 (D.D.C. 2013) (explaining that tower dumps "can capture data associated with thousands of innocent Americans' phones"). Thus, a tower dump—especially one that seeks records from multiple telecommunications carriers over a significant period of time—conveys the sensitive communications records of many parties as to whom the government cannot make *any* showing of suspicion whatsoever. At best, the government is seeking records from individuals who may share a cellular service provider with a potential, unknown criminal suspect. That is plainly not a sufficient showing under the *Terry* "reasonable suspicion" standard.

In fact, the kind of overbroad collection sought by the government here could not even meet the lower standard of mere "relevance" that governs ordinary subpoenas. *See Oxford American Dictionary* 1474 (3d ed. 2010) ("the state of being closely connected or appropriate to the matter in hand"); *Webster's Collegiate Dictionary* 1051 (11th ed. 2012) ("having significant and demonstrable bearing on the matter at hand"). Under the lower "relevance" standard, courts have consistently required that the particular records demanded by the government bear an actual connection to a particular investigation. *See, e.g.*, *Bowman Dairy Co. v. United States*, 341 U.S. 214, 221 (1951) (invalidating a subpoena's "catch-all provision" on the grounds that it was "merely a fishing expedition to see what may turn up"). Courts have also rejected or narrowed subpoenas that, because they fail to identify the outer bounds of the categories of documents they seek, cover large volumes of *irrelevant* documents. *See In re Horowitz*, 482 F.2d 72, 79 (2d Cir. 1973) (Friendly, J.) (narrowing a grand-jury subpoena on the grounds that it improperly demanded the contents of multiple filing cabinets "without any attempt to define classes of potentially relevant documents or any limitations as to subject matter or time period"). Indeed, this Court has quashed a grand-jury subpoena that demanded the entire contents of "computer hard drives and floppy disks," because the materials "contain[ed] some data concededly irrelevant to the grand jury inquiry." *In re Grand Jury Subpoena Duces Tecum Dated Nov. 15, 1993*, 846 F. Supp. 11, 12 (S.D.N.Y. 1994) (Mukasey, J.). If anything, the proposed collection in this case is far broader, and contains far more plainly irrelevant records, than these kinds of cases.

### C. The Stored Communications Act Affords Magistrate Judges Discretion to Deny an Application for an Order Under 18 U.S.C. § 2703(d) and Instead Require the Government to Seek a Probable Cause Warrant.

Even if the government could satisfy § 2703(d)'s reasonable suspicion standard, it does not follow that the Court must grant the government's request for tower-dump data under § 2703(d). Section 2703 provides a sliding scale of mechanisms by which the government may obtain subscriber records from an electronic communication service: an administrative subpoena for specifically enumerated and very limited subscriber information, *id.* § 2703(c)(2), a court order or a warrant for *other* non-content information, *id.* § 2703(c)(1)(A)–(B), and a warrant for the contents of communications, *id.* § 2703(a); *United States v. Warshak*, 631 F.3d 266 (6th Cir.

2010). For the middle category—non-content "record[s] or other information pertaining to a subscriber . . . or customer," 18 U.S.C. § 2703(c)(1)—magistrate judges have discretion to "require a warrant showing probable cause," even where the government has made the factual showing required for an order under § 2703(d). *In Third Circuit Opinion*, 620 F.3d at 315–17, 319.[33] The plain text and legislative history of the statute support this view.

> The relevant text of § 2703(d) states:
>
> A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and *shall issue only if* the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.

18 U.S.C. § 2703(d) (emphasis added). As the Third Circuit has explained, the SCA's use of the phrase "only if" in § 2703(d) indicates that the "specific and articulable facts" showing required by that section is a necessary, but not sufficient condition for the issuance of a § 2703(d) order. *Third Circuit Opinion*, 620 F.3d at 315–16; *accord Williams v. Ward*, 556 F.2d 1143, 1158 n.6 (2d Cir. 1977) (explaining that the statutory language "only if" and "unless" are both "phrased . . . as necessary rather than sufficient conditions"). "If Congress wished that courts 'shall,' rather than 'may,' issue § 2703(d) orders whenever the [statutory] standard is met, Congress could easily have said so. At the very least, the use of 'may issue' strongly implies court discretion, an implication bolstered by the subsequent use of the phrase 'only if' in the same sentence." *Third Circuit Opinion*, 620 F.3d at 315.[34]

Magistrate judges need not automatically issue an order under § 2703(d) without regard to the sensitivity of the information sought. Rather, recognizing that some records that would otherwise be available to the government under the statute may merit higher protection under the Fourth Amendment, Congress provided magistrate judges with the option to deny an application for a § 2703(d) order and instead require a search warrant pursuant to § 2703(c)(1)(A).

Indeed, reading the statute to allow courts to avoid serious constitutional questions—by giving them the discretion to require warrants in cases raising Fourth Amendment concerns—is

---

33 A divided panel of the Fifth Circuit disagrees. *See Fifth Circuit Opinion*, 724 F.3d at 607 ("If the[ statutory] conditions are met, the court does not have the discretion to refuse to grant the order."). *But see id.* at 617 (Dennis, J., dissenting) ("Section 2703(c) may be fairly construed to provide for 'warrant procedures' to be followed when the government seeks customer records that may be protected under the Fourth Amendment, including historical cell site location information.").

34 Congress has elsewhere provided for mandatory issuance of court orders based on a specific legal showing, but it chose not to do so here. *See, e.g.*, 18 U.S.C. § 3123(a)(1) (providing that "the court *shall* enter an ex parte order authorizing the installation and use of a pen register or trap and trace device . . . , *if* the court finds that the attorney for the Government has certified to the court that the information [sought] . . . is relevant to an ongoing criminal investigation" (emphases added)); Fed. R. Crim. P. 41(d)(1) ("After receiving an affidavit or other information, a magistrate judge . . . *must* issue the warrant if there is probable cause to search for and seize a person or property . . . ." (emphasis added)).

compelled by the doctrine of constitutional avoidance. *See Fifth Circuit Opinion*, 724 F.3d at 616–17 (Dennis, J., dissenting) ("[B]ecause the government's interpretation 'give[s] rise to [a] substantial constitutional question[ ],' precedent requires that we 'first ascertain whether a construction of the statute is fairly possible by which the constitutional question may be avoided.'" (first alteration added) (citations omitted)). The constitutional avoidance doctrine "rest[s] on the reasonable presumption that Congress did not intend" any meaning of a statute "which raises serious constitutional doubts," *Clark v. Martinez*, 543 U.S. 371, 381 (2005), and "[i]t is therefore incumbent upon [the Court] to read the statute to eliminate those doubts so long as such a reading is not plainly contrary to the intent of Congress." *United States v. X-Citement Videos, Inc.*, 513 U.S. 64, 78 (1994). As detailed below, at a minimum warrantless acquisition of tower-dump data raises serious constitutional concerns. Therefore, in order to avoid conflict with the Fourth Amendment, this Court should default to the warrant requirement explicitly provided by the statute, and should require the government to demonstrate probable cause.[35]

## II. Although Tower Dumps Likely Violate the Fourth Amendment in All Cases, At the Very Least They May Not Be Conducted Without a Warrant.

### A. A Tower Dump Is a Search Under the Fourth Amendment.

The Supreme Court has made clear that location tracking infringes on reasonable expectations of privacy and therefore constitutes a search under the Fourth Amendment, at least when it is of a "dragnet type" or when it reveals information concerning an individual's location in private places such as the home. The requested tower-dump data in this case would be a search for these reasons. Moreover, the intentional targeting of large numbers of non-suspects is inherently unreasonable under the Fourth Amendment and raises the concerns animating the longstanding prohibition on "general warrants." Even if this Court determines that tower dumps are sometimes permissible under the Fourth Amendment, they are quite clearly unconstitutional when conducted without a warrant. *See Arizona v. Gant*, 556 U.S. 332, 338 (2009) (warrantless searches are "'per se unreasonable'" (quoting *Katz v. United States*, 389 U.S. 347, 357 (1967)). The only federal magistrate judge yet to address the issue in a published opinion has held that the Fourth Amendment requires the government to obtain a warrant for a tower dump. At the very least, this Court should adopt at least that level of protection here. *See Owsley Opinion I*, 930 F. Supp. 2d 698.

In *United States v. Knotts*, 460 U.S. 276 (1983), the Supreme Court held that using a rudimentary tracking device—a beeper—to track a vehicle's movements on public roadways does not constitute a Fourth Amendment search. *Id.* at 281–82. The Court was careful to note, however, that "dragnet type law enforcement" use of beepers would not be permitted by the Court's holding, and that "different constitutional principles may be applicable" there. *Id.* at 284. Courts of appeals have relied on *Knotts* to similarly explain that, whatever the constitutional

35 Although, the ACLU argues below that warrantless requests for tower-dump data violate the Fourth Amendment, this Court need not explicitly rule on the constitutional question in order to apply the warrant requirement. Under the doctrine of constitutional avoidance, the Court need only recognize that warrantless tower dumps raise significant constitutional questions in order to deny the government's application for an order under § 2703(d) and require a warrant under § 2703(c)(1)(A).

status of targeted GPS tracking of a specific suspect, "'wholesale surveillance'" of large numbers of people using GPS devices would raise especially troubling Fourth Amendment concerns. *United States v. Marquez*, 605 F.3d 604, 610 (8th Cir. 2010); *accord United States v. Garcia*, 474 F.3d 994, 998–99 (7th Cir. 2007) (discussing concerns raised by "wholesale surveillance" and "mass surveillance" using GPS trackers); *United States v. Pineda-Moreno*, 617 F.3d 1120, 1126 (9th Cir. 2010) (Kozinski, C.J., dissenting from denial of rehearing en banc) (GPS devices and cell phone location tracking "can provide law enforcement with a swift, efficient, silent, invisible and *cheap* way of tracking the movements of virtually anyone and everyone they choose"); *United States v. Katzin*, 732 F.3d 187, 194 (3d Cir. 2013) (quoting *Knotts*), *reh'g en banc granted, opinion vacated*, No. 12-2548, 2013 WL 7033666 (3d Cir. Dec. 12, 2013).

Tower dumps violate reasonable expectations of privacy under the Fourth Amendment because they involve just the sort of "dragnet type" surveillance of hundreds or thousands of innocent people feared by the Court in *Knotts*. *See In re Application of the United States for an Order Authorizing the Release of Historical Cell-Site Information*, 809 F. Supp. 2d 113, 119 (E.D.N.Y. 2011) (Garaufis, J.) ("[T]he collection of cell-site-location records effectively enables 'mass' or 'wholesale' electronic surveillance, and raises greater Fourth Amendment concerns than a single electronically surveilled car trip."). The reasonable expectation of privacy of cell phone users is that their historical cell phone location information over a period of hours will not be indiscriminately collected by law enforcement without any individualized suspicion of wrongdoing. Even if reasonable suspicion could suffice to justify the search of a *suspect's* historical CSLI, it certainly cannot justify the search of hundreds or thousands of innocent people's location data. As Magistrate Judge Owsley explained, a request for tower-dump data is "a very broad and invasive search affecting likely hundreds of individuals in violation of the Fourth Amendment." *Owsley Opinion I*, 930 F. Supp. 2d at 702; *cf. In re Application for an Order Authorizing Use of a Cellular Telephone Digital Analyzer*, 885 F. Supp. 197, 201 (C.D. Cal. 1995) (denying statutory application to use a cell site simulator device because, *inter alia*, "depending upon the effective range of the digital analyzer, telephone numbers and calls made by others than the subjects of the investigation could be inadvertently intercepted").

Allowing the government to obtain tower-dump data risks sanctioning the sort of "general warrant" that the Fourth Amendment's framers so reviled. *See Stanford v. Texas*, 379 U.S. 476, 481–82 (1965). As the Ninth Circuit observed, requests by "law enforcement for broad authorization to examine electronic records . . . creates a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant." *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1176 (9th Cir. 2010) (en banc) (per curiam); *accord United States v. Galpin*, 720 F.3d 436, 447 (2d Cir. 2013). Surely, a reported gunshot in a residential neighborhood would not allow nonconsensual searches of every home in a several-block radius in hopes of identifying a suspect. Likewise, a theft in Times Square would not permit frisks and bag searches of every person walking along Broadway. Dragnet searches are no more permissible when carried out using electronic means; a claim by the government that a criminal suspect whose email address it does not know sent a potentially incriminating email on a particular day would never authorize it to ask Google or Yahoo to produce a catalogue of every email sent from a New York City internet

protocol address on that day. Grants of "unbridled authority," *Stanford*, 379 U.S. at 481, are unreasonable under the Fourth Amendment, no matter their form.

The government's brief description of the breadth of the tower dump it seeks raises the question of how the records might be used, if not in service of a fishing expedition. The government apparently wants a list of many hundreds or thousands of people nearby any one of multiple cell towers in a New York City neighborhood over a 4.5-hour period. The government provides no public explanation of how it could make use of such a tremendous amount of data, but any use will unnecessarily and unreasonably infringe on the privacy expectations of innocent people. This request is a far cry from the more typical tower dump requests of which the ACLU is aware, where the government is investigating a series of similar crimes and seeks to cross-reference lists of phone users near the locations of those crimes during narrow time windows in order to see whether any one person was present at each scene at the time of each offense. Such a request could at least be structured to minimize the effect on non-suspects (by, for example, using a taint team or requesting that the cell service provider cross-check the lists and provide only a list of potential suspects to the police). The form of the government's request here raises especially acute constitutional concerns.[36]

Although the constitutionality of tower dumps is a difficult question even with a warrant, they are quite clearly unconstitutional when conducted without one. *See Kyllo v. United States*, 533 U.S. 27, 39–40 (2001) (holding that electronic surveillance of heat signatures emanating from a home using technological means "is presumptively unreasonable without a warrant").

The Stored Communications Act provides no means to enforce a particularity requirement via a § 2703(d) order. Kerr, *supra*, at 403. Only by requiring a warrant application that establishes probable cause that the search will uncover evidence of a crime and that "particularly describ[es] the place to be searched," U.S. Const. amend. IV, can this Court constrain the scope of the search as required by the Fourth Amendment. *See United States v. Zemlyansky*, 945 F. Supp. 2d 438, 458 n.5 (S.D.N.Y. 2013) ("The Second Circuit has unequivocally rejected the argument that the particularity requirement should be relaxed when dealing with electronic information."). Such constraints include minimization and retention limitations and a notice requirement to protect the rights of third parties. *See infra* Part II.C (discussing minimization, retention, and notice provisions that a warrant must incorporate).

In addition to raising concerns about dragnets, tower dumps are also searches under the Fourth Amendment because they can reveal facts about constitutionally protected spaces. In *United States v. Karo*, 468 U.S. 705 (1984), the Supreme Court explained that using an electronic device—there, a beeper—to infer facts about "location[s] not open to visual surveillance," like whether "a particular article is actually located at a particular time in the private residence" or to later confirm that the article remains on the premises, was just as unreasonable as searching the location without a warrant. *Id.* at 714–15. Such location tracking,

36 It is worth noting that the most common types of government requests for cell site location information are targeted at the past movements of specific individual suspects. Such requests can be more easily tailored to avoid impacts on third parties, and to comply with the probable cause and particularity requirements of the Fourth Amendment.

the Court ruled, "falls within the ambit of the Fourth Amendment when it reveals information that could not have been obtained through visual surveillance" from a public place, *id.* at 707, regardless of whether it reveals that information directly or through inference. *See also Kyllo*, 533 U.S. at 36 (rejecting "the novel proposition that inference insulates a search," because it is "blatantly contrary" to the Court's holding in *Karo* "where the police 'inferred' from the activation of a beeper that a certain can of ether was in the home").

Like the tracking in *Karo*, cell tower dumps reveal, or enable the government to infer, information about whether cell phones are inside protected locations and whether they remain there. Cell phones travel through many such protected locations where the government cannot intrude without a warrant. *See, e.g. Kyllo*, 533 U.S. at 31 (home); *See v. City of Seattle*, 387 U.S. 541, 543 (1967) (business premises); *Stoner v. California*, 376 U.S. 483, 486–88 (1964) (hotel room). "If at any point a tracked cell phone signaled that it was inside a private residence (or other location protected by the Fourth Amendment), the only other way for the government to have obtained that information would be by entry into the protected area, which the government could not do without a warrant." *Powell*, 943 F. Supp. 2d at 775; *see also Third Circuit Opinion*, 620 F.3d at 318.

This is true even if cell phone location data is less precise than GPS data, because even imprecise information, when combined with visual surveillance or a known address, can enable law enforcement to infer the exact location of a phone. *Third Circuit Opinion*, 620 F.3d at 311. Indeed, that is exactly how the government's experts routinely use such data; "the Government has asserted in other cases that a jury should rely on the accuracy of the cell tower records to infer that an individual, or at least her cell phone, was at home." *Id.* at 311–12. Here, where the density of cell towers in New York City exceeds that of almost any other part of the country, and where the size of cell site sectors is therefore particularly small, cell tower dumps will inevitably reveal extraordinarily precise information about location, including location within homes and other constitutionally protected spaces. This is particularly true of a request covering nighttime hours, when many people will be within their homes. In short, the tower dump sought in this case would undoubtedly constitute a search, and the government therefore must obtain a warrant.

### B. Cell Service Providers' Ability to Access Customers' Location Data Does Not Eliminate Cell Phone Users' Reasonable Expectation of Privacy in that Data.

The government argues that people have no reasonable expectation of privacy in their cell phone location information because that information was conveyed to their cell service providers and was contained in those providers' business records. Gov't Ltr.-Br. at 3–7. However, the Supreme Court cases on which the government relies do not address the bulk surveillance at issue here. And besides, unlike the kinds of records at issue in those cases, people do not voluntarily convey their location information to their wireless carriers. The only two circuits to address that issue have split, with the Third Circuit holding that cell phone users may maintain a reasonable expectation of privacy in their location records even though these records are held by a third party business. *Third Circuit Opinion*, 620 F.3d at 317–18. *But see Fifth Circuit Opinion*, 724 F.3d at 611–15. That is the correct conclusion, and this Court should follow it here.

The government relies on *United States v. Miller*, 425 U.S. 435 (1976), and *Smith v.*

*Maryland*, 442 U.S. 735 (1979), for the claim that there is no reasonable expectation of privacy whatsoever in any records possessed by a third party. But the Supreme Court has yet to decide the question presented by this case: whether the Fourth Amendment permits the government to collect thousands of Americans' location records in bulk. Neither *Miller* nor *Smith* addressed the question presented here, and the Supreme Court's more recent cases only confirm that *Smith* does not have the broad reach the government now attributes to it.

*Smith* resolved a narrow question with a narrow ruling. It held that the Fourth Amendment was not implicated by the government's collection of a single criminal suspect's phone records over a period of several days. *Smith* did not address the question of dragnet surveillance. Indeed, just four years after it decided *Smith*, the Supreme Court explicitly recognized that the distinction between targeted surveillance and dragnet surveillance is a constitutionally significant one. *See Knotts*, 460 U.S. 276. More recently, in *United States v. Jones*, 132 S. Ct. 945 (2012), five Justices observed that a different form of dragnet surveillance—the long-term tracking of an individual in public—amounted to a search under the Fourth Amendment. *Id.* at 964 (Alito, J., concurring in the judgment); *id.* at 955 (Sotomayor, J., concurring); *see also United States v. Maynard*, 615 F.3d 544, 557 (D.C. Cir. 2010), *aff'd sub nom. Jones*, 132 S. Ct. 945. The cardinal question presented here is whether people have a reasonable expectation that their location information will not be subject to dragnet government surveillance. The answer to that question should be derived using the familiar test from *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring), not from cases that do not purport to address the scope and nature of the government's request.

*Smith* and *Miller* do not reach the government surveillance at issue in this case for another reason: They require the voluntary conveyance of information, which is not present here. In *Miller*, the Court held that a bank depositor had no expectation of privacy in records about his transactions that were held by the bank. Although the Court explained that the records were the bank's business records, 425 U.S. at 440, it proceeded to inquire whether the depositor could nonetheless maintain a reasonable expectation of privacy in the records: "We must examine the nature of the particular documents sought to be protected in order to determine whether there is a legitimate 'expectation of privacy' concerning their contents." *Id.* at 442. The Court's ultimate conclusion—that the depositor had no such expectation—turned not on the fact that the records were owned or possessed by the bank, but on the fact that the depositor "voluntarily conveyed" the information contained in them to the bank and its employees. *Id.*

In *Smith*, the Court held that the use of a pen register to capture the telephone numbers an individual dials was not a search under the Fourth Amendment. 442 U.S. at 739, 742. The Court relied heavily on the fact that when dialing a phone number the caller "voluntarily convey[s] numerical information to the telephone company." *Id.* at 744. As in *Miller*, in addition to establishing voluntary conveyance the Court also assessed the invasiveness of the surveillance at issue to determine whether the user had a reasonable expectation of privacy. The Court noted the "pen register's limited capabilities," *id.* at 742, explaining that "'a law enforcement official could not even determine from the use of a pen register whether a communication existed.'" *Id.* at 741 (quoting *United States v. N.Y. Tel. Co.*, 434 U.S. 159, 167 (1977)).

Assessing an individual's expectation of privacy in cell phone location information thus turns on whether the individual voluntarily conveyed the contents of the location records to the wireless provider, and on what privacy interest the person retains in the records. The Third Circuit has persuasively explained why cell phone users retain a reasonable expectation of privacy in their location information:[37]

> A cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way. . . . [I]t is unlikely that cell phone customers are aware that their cell phone providers *collect* and store historical location information. Therefore, "[w]hen a cell phone user makes a call, the only information that is voluntarily and knowingly conveyed to the phone company is the number that is dialed and there is no indication to the user that making that call will also locate the caller; when a cell phone user receives a call, he hasn't voluntarily exposed anything at all."

*Third Circuit Opinion*, 620 F.3d at 317–18 (last alteration in original).

There is nothing inherent in the placing of a cell phone call that would indicate to callers that they are exposing their *location* information to their wireless carrier. In both *Miller* and *Smith*, the relevant documents and dialed numbers were directly and voluntarily conveyed to bank tellers and telephone operators, or their automated equivalents. *See*, *e.g.*, *Smith*, 442 U.S. at 744. But when a cell phone user makes or receives a call, there is no indication that making or receiving the call will also create a record of the caller's location. The user does not input her location information into the phone, and the phone does not notify the user that her location has been logged. Moreover, unlike the dialed phone numbers at issue in *Smith*, location information does not appear on a typical user's monthly bill. *See id.* at 742.

Further, the government's lengthy discussion of smartphone "apps" is inapt. *See* Gov't Ltr.-Br. at 3 n.2. Most smartphones have an opt-in permission system, in which apps can only obtain location data if a user chooses to consent to such access when installing or enabling the app.[38] Many smartphones also have an overarching location privacy setting that, when enabled, prevents all apps on the phone from accessing the phone's location. However, these settings have

---

37 The government incorrectly asserts that the Third Circuit has "held that the Fourth Amendment is not implicated by an order requiring a phone company to provide cell site data to the Government." Gov't Ltr.-Br. at 6. In fact, the Third Circuit rejected application of the third party doctrine to CSLI, characterized the government's position that there is no privacy interest in the location of cell phones within private homes as "extreme," and concluded that magistrate judges have discretion to require warrants for CSLI so long as they "make fact findings and give a full explanation." *Third Circuit Opinion*, 620 F.3d at 317–19.

38 *See*, *e.g.*, Apple, *Apple Q&A on Location Data* (Apr. 27, 2011), https://www.apple.com/pr/library/2011/04/27Apple-Q-A-on-Location-Data.html ("[The iPhone] ask[s] users to give their permission for each and every app that want[s] to use location."). The Federal Trade Commission requires app developers to disclose clearly and prominently to users that they are collecting and utilizing location information, and has brought enforcement actions against companies that collect location information without explicit user consent. *See, e.g.*, Cecilia Kang, *Flashlight App Kept Users in the Dark about Sharing Location Data: FTC*, Wash. Post., Dec. 5, 2013, http://www.washingtonpost.com/business/technology/flashlight-app-kept-users-in-the-dark-about-sharing-location-data-ftc/2013/12/05/1be26fa6-5dc7-11e3-be07-006c776266ed_story.html.

no impact at all upon *carriers'* ability to learn the cell sector in use, thus potentially misleading phone users. Cell site location information is automatically determined by the wireless provider but is not actively, intentionally, or affirmatively disclosed by the caller.[39]

Moreover, contrary to the government's assertion, *see* Gov't Ltr.-Br. at 6, the existence of privacy policies on cell service providers' websites does nothing to convert automatic, involuntary retention of location information into voluntary conveyance of such data. The policies cited by the government provide limited discussion of the location data automatically stored by service providers, and do not specify a length of time the information is retained. The government makes no showing that any of the thousands of people whose records it seeks are actually aware of these privacy policies, much less that they read or understood them. *Cf.* M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 Notre Dame L. Rev. 1027, 1032 & n.34 (2012) (noting that most consumers do not read privacy policies). Even if cell phone users are aware of the policies' existence, it is likely that they would think the privacy policies would *protect against* collection and disclosure of information, not facilitate it.[40] Indeed, privacy policies misleadingly suggest that whatever location information is collected is subject to robust confidentiality protections. *See, e.g.*, MetroPCS Privacy Policy[41] ("Under federal law, you have a right, and we have a duty, to protect the confidentiality of [customer proprietary network information] and we have adopted policies and procedures designed to ensure compliance with those rules.").

Finally, the fact that cell phone location information is handled by a third party is not dispositive. The Sixth Circuit's opinion in *Warshak* is instructive. There, the court held that there is a reasonable expectation of privacy in the contents of emails. The court explained that the fact that email is sent through an internet service provider's servers does not vitiate the legitimate interest in email privacy: Both letters and phone calls are sent via third parties (the postal service and phone companies), but people retain a reasonable expectation of privacy in those forms of communication. 631 F.3d at 285 (citing *Katz*, 389 U.S. at 353; *United States v. Jacobsen*, 466 U.S. 109, 114 (1984)). *Warshak* further held that even if a company has a right to access information in certain circumstances under the terms of service (such as to scan emails for viruses or spam), that does not necessarily eliminate the customer's reasonable expectation of privacy vis-à-vis the government. *Id.* at 286–88. In a variety of contexts under the Fourth Amendment, access to a protected area for one limited purpose does not render that area suddenly unprotected from government searches. *See, e.g.*, *Stoner*, 376 U.S. at 487–90 (implicit consent to janitorial personnel to enter motel room does not amount to consent for police to search room); *Chapman v. United States*, 365 U.S. 610, 616–17 (1961) (search of a house invaded tenant's Fourth Amendment rights, even though landlord had

39 The government's mention of dropped calls and of cell phones' displays of "bars representing the strength of the signal" does not aid its argument. *See* Gov't Ltr.-Br. at 5–6. Neither of these points establishes that people voluntarily convey their location information to their cell service providers, nor that they have any information about whether providers log and retain location information or how accurate such location information might be.

40 *See* Joseph Turrow et al., *Research Report: Consumers Fundamentally Misunderstand the Online Advertising Marketplace* 1 (2007), *available at* http://www.law.berkeley.edu/files/annenberg_samuelson_advertising.pdf (reporting that most people think the mere existence of a privacy policy on a website means "the site will not share my information with other websites or companies").

41 http://www.metropcs.com/metro/tac/termsAndConditions.jsp?terms=Privacy%20%20Policy.

authority to enter house for some purposes).

Like the contents of emails, cell phone location information is not a simple business record voluntarily conveyed by the customer. In this case the government seeks location records for hundreds or thousands of innocent, unwitting people. This Court should heed the Supreme Court's caution that new technologies should not be allowed to "erode the privacy guaranteed by the Fourth Amendment." *Kyllo*, 533 U.S. at 34; *see also Warshak*, 631 F.3d at 285 ("[T]he Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish.").

### C. Any Warrant Issued for Tower-Dump Data Must Include Minimization, Retention, and Notice Requirements.

If this Court determines that the Fourth Amendment and § 2703(c) permit tower dumps in some circumstances and directs the government to seek a warrant, the Court must ensure that any warrant issued complies with the Fourth Amendment's particularity and notice requirements. A warrant for tower-dump data will be valid only if based on probable cause, and only if—at a minimum—it requires minimization of the amount of innocent third parties' data collected, restricts retention of such data after the search, and mandates notice to all persons whose cell phone location information the government has obtained.

The Second Circuit has explained that there is a "heightened sensitivity to the particularity requirement in the context of digital searches." *Galpin*, 720 F.3d at 447. Digital searches must be constrained by courts, in part because "files containing evidence of a crime may be intermingled with millions of innocuous files." *Id.* Indeed, there is "a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant." *Id.* (quoting *Comprehensive Drug Testing, Inc.*, 621 F.3d at 1176).

As the Ninth Circuit has explained, "the threat to the privacy of innocent parties from a vigorous criminal investigation" is heightened when sensitive data of multiple individuals is intermingled in electronic storage. *Comprehensive Drug Testing, Inc.*, 621 F.3d at 1175.

> [This danger] calls for greater vigilance on the part of judicial officers in striking the right balance between the government's interest in law enforcement and the right of individuals to be free from unreasonable searches and seizures. The process of segregating electronic data that is seizable from that which is not must not become a vehicle for the government to gain access to data which it has no probable cause to collect.

*Id.* at 1177. Thus, when a search has the potential to sweep up information that does not pertain to the suspect under investigation or is not justified by the government's showing of probable cause, "ex ante instructions are sometimes acceptable mechanisms for ensuring the particularity of a search." *In re Appeal of Application for Search Warrant*, 71 A.3d 1158, 1170 (Vt. 2012); *accord In re Search of Info. Associated with the Facebook Account Identified by Username Aaron.Alexis that is Stored at Premises Controlled by Facebook, Inc.*, No. 13-MJ-742 (JMF), __

F. Supp. 2d __, 2013 WL 7856600, at *7 (D.D.C. Nov. 26, 2013) (Facciola, M.J.) ("This Court will insist, however, that some safeguards must be put in place to prevent the government from collecting and keeping indefinitely information to which it has no right.").

As one magistrate judge has explained, the "failure to address the privacy rights for the Fourth Amendment concerns of . . . innocent subscribers whose information will be compromised as a request of the cell tower dump is another factor warranting the denial" of an application for a tower dump. *Owsley Opinion I*, 930 F. Supp. 2d at 702. In light of these concerns, this Court should, at a minimum, place the following restrictions on any warrant it issues for a cell tower dump:

- **Minimization of the number of innocent persons' location information and call records obtained.** In a crucial respect, the Court can ensure a constitutionally acceptable level of particularity by narrowing the time period covered by the government's request. *See Owsley Opinion II*, 945 F. Supp. 2d at 771. The length of time covered by a tower dump authorization must be narrowly tailored to the crime under investigation; there must be a nexus between the government's probable cause showing and the timespan of the request. Although it may not be possible to set a firm across-the-board limit on the timespan of tower dumps, courts can look for guidance to the "typical" length of tower dump requests that cell service providers receive: 30 minutes.[42]

  To the same end, the Court could order the use of a "taint team," or an entity separate from the investigating officer, to scrutinize the tower dump records, identify records pertaining to a criminal suspect as to whom the government has probable cause, and forward only those records to the criminal investigative team. *See Comprehensive Drug Testing, Inc.*, 621 F.3d at 1171 ("The government also failed to comply with another important procedure specified in the warrant, namely that 'computer personnel' conduct the initial review of the seized data and segregate materials not the object of the warrant for return to their owner."); *id.* at 1180 (Kozinski, C.J., concurring) ("Segregation and redaction of electronic data must be done either by specialized personnel or an independent third party."); *In re Appeal of Application for Search Warrant*, 71 A.3d at 1174–82.[43]

- **Limitations on the retention of any data and records pertaining to innocent third parties that the government obtains in the tower dump.** As soon as practicable after the government has reviewed the tower dump records, it should be required to "return any and all original records and copies, whether hardcopy or in electronic format or storage,

42 *See* Letter from Verizon Wireless to Senator Edward J. Markey, *supra*.

43 *Cf. United States v. Grant*, No. 04 CR 207BSJ, 2004 WL 1171258 (S.D.N.Y. May 25, 2004) (endorsing government's proposed "privilege team" to screen seized documents for privileged materials); *United States v. Triumph Capital Grp., Inc.*, 211 F.R.D. 31, 43 (D. Conn. 2002) ("The use of a taint team is a proper, fair and acceptable method of protecting privileged communications when a search involves property of an attorney."); *United States v. Hunter*, 13 F. Supp. 2d 574, 583 (D. Vt. 1998) (accepting the use of "screening procedure designed by the government" in order to "limit invasion of confidential or privileged or irrelevant material"). (Citations and parentheticals taken from *In re Appeal of Application for Search Warrant*, 71 A.3d at 1179).

to the Provider, which are determined to be not relevant to the Investigative Agency's investigation." *Owsley Opinion II*, 945 F. Supp. 2d at 771. The government should not be permitted to retain location records of hundreds or thousands of innocent people as to whom there is no probable cause. *See Comprehensive Drug Testing, Inc.*, 621 F.3d at 1180 (Kozinski, C.J., concurring) ("The government must destroy or, if the recipient may lawfully possess it, return non-responsive data, keeping the issuing magistrate informed about when it has done so and what it has kept.").

- **Limitation on the government's ability to rely on the plain view doctrine.** If the government is permitted to obtain tower-dump data that contains innocent third parties' records, it should be barred from using those records for any other investigation or purpose. In the context of searches of electronic data on a computer, the Second Circuit has directed that a "district court's review of the plain view issue should take into account the degree, if any, to which digital search protocols target information outside the scope of the valid portion of the warrant. To the extent such search methods are used, the plain view exception is not available." *Galpin*, 720 F.3d at 451. Eliminating the availability of the plain view doctrine will help ensure that the tower dump does not become a suspicionless fishing expedition into the private records of large numbers of third parties with far-reaching collateral consequences.

- **Required notice to all persons whose cell phone location records are included in the tower dump.** Without receiving notice, affected persons—particularly non-suspects—will have no way to learn that they have been subjected to a search and no opportunity to vindicate any violation of their constitutional rights. Notice of a government search is required by Rule 41. *See* Fed. R. Crim. P. 41(f)(1)(C). Failure to provide notice also "casts strong doubt on [a warrant's] constitutional adequacy." *United States v. Freitas*, 800 F.2d 1451, 1456 (9th Cir. 1986) (citing *Berger v. New York*, 388 U.S. 41, 60 (1967)); *see also United States v. Villegas*, 899 F.2d 1324, 1337 (2d Cir. 1990) ("[I]f a delay in notice is to be allowed, the court should nonetheless require the officers to give the appropriate person notice of the search within a reasonable time after the covert entry."). As the Ninth Circuit has explained, "[a] warrant [i]s constitutionally defective [if it] fail[s] to provide explicitly for notice within a reasonable, but short, time subsequent to the surreptitious entry. . . . We take this position because surreptitious searches and seizures of intangibles strike at the very heart of the interests protected by the Fourth Amendment." *Freitas*, 800 F.2d at 1456. Accordingly, at least one magistrate judge has issued a warrant authorizing a tower dump only on the condition that "there will be delayed notification by the providers to subscribers that they have provided records to the Government pursuant to a court order." *Owsley Opinion II*, 945 F. Supp. 2d at 771.

- **Demonstration that other investigative procedures have been exhausted.** Because of a tower dump's effect on the privacy interests of large numbers of non-suspects, the Court should only authorize a tower dump after the government certifies that it has exhausted other investigative methods. *Cf.* 18 U.S.C. § 2518(1)(c) **(**requiring the government to explain "whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous").

Tower dumps raise serious privacy concerns. If they are to be allowed at all, they should be allowed only pursuant to a probable cause warrant that strictly limits the impact on the rights of third parties, as outlined above.

## CONCLUSION

For the foregoing reasons, the Court should deny the government's request for a tower dump as not permitted by the Stored Communications Act, 18 U.S.C. § 2702–03, or the Fourth Amendment. In the alternative, the Court should deny the government's request for an order under § 2703(d) and require it to apply for a probable cause warrant pursuant to § 2703(c)(1)(A) instead.

Respectfully Submitted,

Nathan Freed Wessler
Brett Max Kaufman
Alex Abdo
Ben Wizner
Catherine Crump
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
Phone: 212-549-2500
Fax: 212-549-2654
nwessler@aclu.org

Christopher T. Dunn
Arthur N. Eisenberg
New York Civil Liberties Union Foundation
125 Broad Street, 19th Floor
New York, NY 10004
Phone: (212) 607-3300
Fax: (212) 607-3318
cdunn@nyclu.org

cc: Jason A. Masimore, AUSA
jason.masimore@usdoj.gov