NO. 11-20884

IN THE

UNITED STATES COURT OF APPEALS FOR THE FIFTH CIRCUIT

IN RE: APPLICATIONS OF THE
UNITED STATES OF AMERICA
FOR HISTORICAL CELL-SITE DATA

On Appeal from the United States District Court
For the Southern District of Texas
Houston Division, Civil No. 4:11-MC-00223
Related Cases: 4:10-MJ-981, 4:10-MJ-990, 4:10-MJ-998

BRIEF FOR THE UNITED STATES

KENNETH MAGIDSON
United States Attorney

RENATA A. GOWIE
Chief, Appellate Division

LANNY A. BREUER
Assistant Attorney General

NATHAN JUDISH
Senior Counsel
Computer Crime and Intellectual Property Section
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530
(202) 616-7203

STATEMENT REGARDING ORAL ARGUMENT

The government requests oral argument, as it may be helpful to the Court in addressing the novel issues presented by this appeal.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

RULES

OTHER AUTHORITIES

NO. 11-20884

IN THE
UNITED STATES COURT OF APPEALS
FOR THE FIFTH CIRCUIT

IN RE: APPLICATIONS OF THE
UNITED STATES OF AMERICA
FOR HISTORICAL CELL-SITE DATA

On Appeal from the United States District Court
For the Southern District of Texas
Houston Division, Civil No. 4:11-MC-00223
Related Cases: 4:10-MJ-981, 4:10-MJ-990, 4:10-MJ-998

BRIEF FOR THE UNITED STATES

STATEMENT OF JURISDICTION

This case is a direct appeal from the decision and Order of the district court denying an appeal by the United States of three separate orders by a magistrate judge. The magistrate judge's three orders denied applications of the United States under 18 U.S.C. § 2703(d) for orders to obtain historical cell-site records. The district court had jurisdiction pursuant to 28 U.S.C. § 636 and 18 U.S.C. § 2703(d). The United States filed a timely notice of appeal to this Court on December 12, 2011. (R. 52).

This Court has jurisdiction under 28 U.S.C. § 1291.[1] In the event that this Court concludes that it lacks jurisdiction under § 1291, however, the United States submits that this Court should review the order by way of mandamus under 28 U.S.C. § 1651.

STATEMENT OF THE ISSUES

1. Whether the district court erred in holding the Stored Communications Act, 18 U.S.C. § 2703, unconstitutional because the Act allows the United States to obtain a court order compelling a cell phone company to disclose historical cell-site records created and kept by the company in its ordinary course of business, where such order is based on a showing of "specific and articulable facts" that there are reasonable grounds to believe that the records sought are relevant and material to an ongoing criminal investigation.

---

[1] In *In re Application of the United States*, 620 F.3d 304 (3d Cir. 2010), the Third Circuit reviewed a district court order similar to the one in this case. Although the Third Circuit did not explicitly identify its basis for jurisdiction, it appears to have proceeded under 28 U.S.C. § 1291. It stated that "[w]e have de novo review" and cited as support a case in which the court's jurisdiction was based on § 1291. *See In re Application of the United States*, 620 F.3d at 305 (citing *DIRECTV Inc. v. Seijas*, 508 F.3d 123, 125 (3d Cir. 2007)). In addition, two appellate courts have held that an appeal lies under § 1291 if a district court denies an application under 18 U.S.C. § 2518 for a Title III order to intercept communications. *See In re Application of the United States*, 563 F.2d 637, 641 (4th Cir. 1977); *Application of the United States*, 427 F.2d 639, 642 (9th Cir. 1970). The Fourth Circuit explained that a Title III application is "not filed in a pending trial or criminal proceeding, but rather in an independent plenary proceeding" pursuant to statute, and "the order of the district court denying the application was dispositive thereof and had the requisite finality to make it appealable under section 1291." *In re Application of the United States*, 563 F.2d at 641. This reasoning applies equally to an application for a 2703(d) order.

2. Whether the district court erred in overruling the government's objections to the magistrate judge's judicially-noticed "findings of fact" about location information generated and stored by cell phone companies, where those findings were disputed by the United States and contradicted by a sworn affidavit from a cell phone provider.

STANDARDS OF REVIEW

The district court's conclusions of law on Fourth Amendment issues are reviewed de novo, and its findings of fact are reviewed for clear error. *See United States v. Gomez-Moreno*, 479 F.3d 350, 354 (5th Cir. 2007). A district court's use of judicial notice under Federal Rule of Evidence 201 is reviewed for abuse of discretion. *See Taylor v. Charter Medical Corp.*, 162 F.3d 827, 829 (5th Cir. 1998).

STATEMENT OF THE CASE

On October 5, 6, and 12, 2010, in three separate criminal investigations, the United States filed similar applications for court orders under 18 U.S.C. § 2703(d) ("2703(d) orders") to compel cell phone companies to produce historical cell-site information (as well as other records) for specified phones. (A. 1-12, 17-31, 37-48).[2]

[2] These three applications received three separate docket numbers: 4:10-mj-981, 4:10-mj-990, and 4:10-mj-998. After the government filed and briefed its appeal from the magistrate judge's order to the district court, the government's appeal to the district court was assigned a new docket number: 4:11-mc-00223. When the government appealed the district court's order to this Court, the record on appeal initially included only entries from the district court docket. On February 13, 2012, this Court granted the government's motion to supplement the record with the docket sheets

The first and third applications sought orders directed to T-Mobile; the second sought an order directed to MetroPCS. On the day each application was filed, Magistrate Judge Stephen Smith issued an order denying the application for historical cell-site information but granting the application for other specified subscriber information. (A. 13-16, 32-36, 49-52).

On October 14, 2010, the magistrate judge issued an order directing the United States to file a brief addressing its applications for historical cell-site records in these three cases. (A. 53-54). The United States did so on October 25, 2010. (A. 55-79). On October 29, 2010, the magistrate judge issued an opinion denying the government's applications and declaring that "[c]ompelled warrantless disclosure of cell site data violates the Fourth Amendment." *In re Application of the United States for Historical Cell Site Data*, 747 F. Supp. 2d 827, 846 (S.D. Tex. 2010) (hereinafter, *Magistrate Judge Opinion*).

The United States sought review in the district court. (A. 80-112). On November 11, 2011, the district court (Judge Lynn Hughes) issued a one-page order

---

in the three magistrate judge cases. As the supplemented record is not yet available for citation, the government is submitting with this brief an Appendix that includes relevant documents from the magistrate judge dockets. In this brief, citations of the form "(A. n)" are to this Appendix. Citations of the form "(R. n)" are to the initial record on appeal from the district court docket. This Appendix is filed under seal because the three applications and magistrate judge orders (A. 1-52) concern pending investigations and are under seal in the district court.

overruling the United States's objections to the *Magistrate Judge Opinion* and stating that the *Magistrate Judge Opinion* "subsists." (R. 43). This appeal followed.

STATEMENT OF FACTS

A. The Stored Communications Act

Under 18 U.S.C. § 2703(c)(1), the United States 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)" when it obtains a 2703(d) order. A court issues a 2703(d) order when the government provides "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).

B. The Government's Applications for 2703(d) Orders

On October 5, 6, and 12, 2010, the United States filed similar applications in separate investigations for 2703(d) orders to compel cell phone companies to produce historical cell-site information (as well as other records) for targeted phones in three separate investigations. First, on October 5, the United States submitted an application for a 2703(d) order to compel cell phone service provider T-Mobile to disclose, among various classes of information for a specified subscriber's phone,

historical cell-site information for a specified sixty-day period. (A. 1-12). In the application, the applicant Assistant United States Attorney ("AUSA") set forth facts explaining that the target cell phone was used by a specified individual to arrange for the transportation and distribution of illegal drugs in the Houston area. (A. 8-11).

Second, on October 6, the United States submitted an application for a 2703(d) order to compel cell phone service provider MetroPCS to disclose historical cell-site and other records for a customer's phone for a specified sixty-day period. (A. 17-31). The applicant AUSA set forth facts explaining that the targeted cell phone was used by a specified individual who was a head of an organization involved in drug trafficking, undocumented alien smuggling, and bribery of public officials. (A. 24-30).

Third, on October 12, the United States applied for a 2703(d) order to compel T-Mobile to disclose historical cell-site and other records for a specified phone for a specified sixty-day period. (A. 37-48). The applicant AUSA set forth facts explaining that the phone was in the possession of a gang member and had been used to schedule gang meetings, coordinate gang activity, and facilitate robbery and extortion. (A. 44-47).

Each application sought "historical cellsite information and call detail records (including in two-way radio feature mode)" for a sixty-day period, and each defined

cell-site information as "the antenna tower and sector to which the cell phone sends its signal." (A. 2, 18, 38). The applications defined "call detail records" to include "the cellsite/sector(s) used by the mobile telephone to obtain service for a call or when in an idle state." (A. 2, 18, 38). Before the district court, the United States subsequently stated that it "now believes that cell phone service providers do not create cell-site records when a phone is in an idle state" and that it "is willing to exclude such information from the scope of its application." (A. 81 n.2).

On the day each application was filed, Magistrate Judge Stephen Smith issued an order denying the application for historical cell-site information but granting the application for other specified subscriber information. (A. 13-16, 32-36, 49-52). For each application, the magistrate judge made a factual finding that the United States had "offered specific and articulable facts showing reasonable grounds to believe that the customer information described below is relevant and material to an ongoing criminal investigation." (A. 13, 32-33, 49). In each case, however, the magistrate judge also held that for historical cell-site information, the Fourth Amendment "demand[s] a higher standard of proof than the specific and articulable facts standard of § 2703." (A. 14, 33, 50).

C. Proceedings before the Magistrate Judge and the Magistrate Judge's Opinion

On October 14, 2010, the magistrate judge ordered the United States to submit a brief regarding its applications, and the magistrate judge also noted his intent to take judicial notice from certain categories of facts, including "congressional testimony at recent hearings before House and Senate committees on ECPA reform." (A. 53-54). The magistrate judge invited the United States to make objections or proposed additions "to these categories of judicially noticed facts." (A. 54). However, the magistrate judge did not provide notice to the United States of any particular facts of which he intended to take judicial notice. In its brief filed on October 25, 2010, the United States responded that it "cannot determine from the broad categories cited by the Court whether it is appropriate to take judicial notice of any particular facts that might fall within those categories." (A. 77).

With its October 25 brief, the United States submitted a redacted sample of historical cell-site information produced by T-Mobile. (A. 79). The sample demonstrated that T-Mobile produced the following information for each call: (1) date and time of call initiation, answer, and termination; (2) the telephone numbers involved in the call, as well as other identifying numbers (IMEI and IMSI) associated with the target phone; (3) whether the call originated or terminated with the target phone; (4) the cell tower to which the customer connected at the beginning

of the call; (5) the cell tower to which the customer was connected at the end of the call; and (6) the duration of the call. (A. 79).

On October 29, 2010, the magistrate judge issued an opinion denying the government's applications and declaring that "[c]ompelled warrantless disclosure of cell site data violates the Fourth Amendment." *Magistrate Judge Opinion*, 747 F. Supp. 2d at 846. The opinion begins with fifty paragraphs of judicially-noticed "findings of fact" that address the structure of phone companies' cellular networks, the accuracy of the location information generated by phone companies, and the kind of location information stored and retained by service providers. *See id.* at 831-35. These "findings of fact" were largely based on statements made before Congress by Matt Blaze, an Associate Professor of Computer and Information Science at the University of Pennsylvania. *See id.* at 831-34 (citing Blaze's testimony in footnotes 13-17, 19, 21-35, 37-40, 42-46, and 51-55). The court asserted that these findings were "appropriate for judicial notice under *Rule 201 of the Federal Rules of Evidence*." *Magistrate Judge Opinion*, 747 F. Supp. 2d at 831.

The findings include claims that "a provider can pinpoint the phone's latitude and longitude to an accuracy within 50 meters or less," that carriers create records "that include the most accurate location information available to them," and that historical cell-site data "is sufficient to plot the target's movements hour by hour for

the duration of the 60 day period covered by the government's request." *Id.* at 833-35 (¶¶ 27, 31, 49). The findings of fact make generic assertions about "some" carriers or "most" carriers, and sometimes make assertions about carriers other than T-Mobile or MetroPCS, but they make no specific mention of T-Mobile or MetroPCS. *Id.* at 833-35 (¶¶ 33, 35, 39).

The *Magistrate Judge Opinion* then addressed the constitutionality of compelled disclosure of historical cell-site records. It rejected application of the Supreme Court's cases concerning compelled disclosure of business records, asserting that cell-site information was not "voluntarily conveyed" to a provider and that "[i]f the telephone numbers dialed in *Smith v. Maryland* were notes on a musical scale, the location data sought here is a grand opera." *Magistrate Judge Opinion*, 747 F. Supp. 2d at 843-46. It then analyzed the compelled disclosure of cell-site records under the legal standards courts have used for information gained from tracking devices surreptitiously installed by the government. It held that "[c]ompelled warrantless disclosure of cell-site data violates the Fourth Amendment under the separate authorities of [*United States v. Karo*, 468 U.S. 705 (1984)] and [*United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010), *aff'd on other grounds sub nom. United States v. Jones*, ___ U.S. ___, 2012 WL 171117 (S. Ct. Jan. 23, 2012)]." *Magistrate Judge Opinion*, 747 F. Supp. 2d at 846.

D. Proceedings Before the District Court and the District Court Order

The United States sought review in the district court. With its brief for the district court, the United States submitted an affidavit from MetroPCS regarding its historical cell-site records. (A. 110-12). The affidavit stated that the average MetroPCS "towers have a coverage radius of about one to two miles," that the radius is "no smaller than 100 yards in some densely populated urban areas," that MetroPCS stores only a record of a single tower the phone was connected to at the beginning and end of the call, that MetroPCS does not store cell-site records when a phone is idle, and that its records "do[] not currently establish the telephone's location with precision." (A. 110-12). In addition, the United States stated that T-Mobile declined to submit an affidavit regarding its historical cell-site records. (A. 84). The United States suggested a hearing if the Court wished to make factual findings regarding the precision of T-Mobile's historical cell-site records and stated that the United States believed that T-Mobile would provide information similar to MetroPCS regarding its historical cell-site information. (A. 85, 89, 109).

On November 11, 2011, the district court (Judge Lynn Hughes) issued a one-page order overruling the United States's objections to the *Magistrate Judge Opinion* and stating that the *Magistrate Judge Opinion* "subsists." (R. 43). The district court provided only minimal Fourth Amendment analysis. The court stated:

> When the government requests records from cellular services, data disclosing the location of the telephone at the time of particular calls may be acquired only by a warrant issued on probable cause. U.S. Const., amend. 4. The records would show the date, time, called number, and location of the telephone when the call was made. These data are constitutionally protected from this intrusion. The standard under the Stored Communications Act, 18 U.S.C. § 2703(d), is below that required by the Constitution.

(R. 43).

SUMMARY OF ARGUMENT

1. Section 2703 of the Stored Communications Act, 18 U.S.C. § 2703, permits the United States to obtain a 2703(d) order compelling a cell phone provider to disclose historical cell-site records, which are the company's records of the cell towers it uses to transmit and receive customers' calls. The government's use of a 2703(d) order to compel disclosure of historical cell-site records is consistent with the Fourth Amendment because a customer has no privacy interest in cell-site records, which are business records created and stored by a cell phone provider in its ordinary course of business.

The Supreme 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." *Smith v. Maryland*, 442 U.S. 735, 744 (1979) (quoting *United States v. Miller*, 425 U.S. 435, 443 (1976)). T-Mobile and MetroPCS inform customers that they collect customer location information, and the customers have

neither ownership, possession, nor control over the providers' historical cell-site records. Because customers have no reasonable expectation of privacy in historical cell-site records created and maintained by T-Mobile and MetroPCS, the district court's order should be reversed and remanded with instructions to grant the government's applications.

Moreover, a 2703(d) order for cell-site records is, like a subpoena, a form of compulsory process, and the Fourth Amendment sets a reasonableness standard rather than a warrant requirement for compulsory process. The Supreme Court has long held that "the Fourth [Amendment], if applicable [to a subpoena], at the most guards against abuse only by way of too much indefiniteness or breadth in the things required to be 'particularly described,' if also the inquiry is one the demanding agency is authorized by law to make and the materials specified are relevant." *Oklahoma Press Publishing Co. v. Walling*, 327 U.S. 186, 208 (1946). Compulsory process authority is critical to the truth-seeking function of the criminal justice process: "[t]o ensure that justice is done, it is imperative to the function of courts that compulsory process be available for the production of evidence needed either by the prosecution or by the defense." *United States v. Nixon*, 418 U.S. 683, 709 (1974). Because there is no probable cause standard for compulsory process, the district

court's order should be reversed and remanded with instructions to grant the government's applications.

In the alternative, there is an additional reason why use of a 2703(d) order to compel disclosure of cell-site records does not violate the Fourth Amendment, although this basis would require a remand to the district court for further factual findings. Even under the standards applicable to surreptitiously installed tracking devices, the Fourth Amendment does not bar compelled disclosure of historical cell-site records. Before the district court, the United States submitted an affidavit from MetroPCS stating that its cell-site records cannot locate a cell phone with precision, and it suggested a hearing to obtain similar testimony from T-Mobile. Under these facts, obtaining historical cell-site records using a 2703(d) order is consistent with the Fourth Amendment's standards for tracking devices: historical cell-site records are not sufficiently precise to reveal a particular private location in which a cell phone may be found or to reveal a comprehensive record of a person's public movements. Moreover, there is no trespass or physical intrusion on a customer's cell phone when the government obtains historical cell-site records from a provider.

2. The only factual findings concerning the accuracy of historical cell-site records made by the magistrate judge or the district court are the magistrate judge's "findings of fact," but these findings must be rejected because they are subject to

dispute and thus inappropriate for judicial notice. The magistrate judge abused his discretion in relying on judicial notice to make "findings of fact" concerning the location information created and stored by service providers and the accuracy of that location information, because "judicial notice applies to self-evident truths that no reasonable person could question, truisms that approach platitudes or banalities." *Hardy v. Johns-Manville Sales Corp.*, 681 F.2d 334, 347 (5th Cir. 1982). The United States believes that the magistrate judge's "findings of fact" are fundamentally inaccurate, but in any case, they are certainly subject to reasonable dispute. They are contradicted by the sworn affidavit from MetroPCS, and they are contrary to previous findings of other courts and the FCC.

ARGUMENT

I. THE FOURTH AMENDMENT ALLOWS THE UNITED STATES TO OBTAIN A 2703(d) ORDER TO COMPEL A CELL PHONE COMPANY TO DISCLOSE HISTORICAL CELL-SITE RECORDS.

A. **A cell phone customer has no privacy interest in historical cell-site records because they are business records created and held by a cell phone provider.**

A historical cell-site record is a phone company's record of the cell tower and sector it used to handle a customer's call. It is a business record generated and stored by a cell phone company at its own discretion. No federal law mandates that a phone

company create or keep historical cell-site records.[3] Indeed, even the *Magistrate Judge Opinion* does not dispute that historical cell-site records are "generated in the ordinary course of the provider's business." *Magistrate Judge Opinion*, 747 F. Supp. 2d at 841. A customer has no Fourth Amendment privacy interest in business records created and held by a third party. Thus, the district court erred in holding that using a 2703(d) order to compel disclose of historical cell-site records violates the Fourth Amendment.

1. A customer has no reasonable expectation of privacy in historical cell-site records.

a. *United States v. Miller*

In *United States v. Miller*, 425 U.S. 435 (1976), the Supreme Court rejected a Fourth Amendment challenge to a third-party subpoena for bank records and explained that the bank's records "are not respondent's 'private papers'" but are "the business records of the banks" in which a customer "can assert neither ownership nor possession." *Miller*, 425 U.S. at 440. The records "pertain to transactions to which the bank was itself a party." *Id.* at 441. In rejecting the challenge to the subpoena, the Court held "that the Fourth Amendment does not prohibit the obtaining of

[3]Pursuant to 47 C.F.R. § 42.6, providers are required to maintain for 18 months "the name, address, and telephone number of the caller, telephone number called, date, time and length of the call." This requirement does not extend to cell-site information.

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." *Miller*, 425 U.S. at 443.

The reasoning of *Miller* also applies to historical cell-site records. First, cell-site records are not a customer's private papers. Once a customer places a call, she thereafter has no control over cell-site records relating to her phone. Moreover, although a customer is likely to be aware that the cell phone company will assign a cell tower to handle her call, the customer typically does not know which cell tower is assigned to process her calls. Second, cell-site records are business records of the provider. The choice to create and store historical cell-site records is made by the provider, and the provider controls the format, content, and duration of the records it chooses to create and retain. Indeed, because cell-site records are not in the possession of a customer, a customer could not be expected to produce cell-site records in response to a subpoena. Third, cell-site records pertain to transactions to which the cell phone company was a party. The assignment of a particular cell tower to process a call is made by the cell phone company to facilitate the functioning of its network. Thus, under *Miller*, a customer's historical cell-site records are not

protected by the Fourth Amendment because they are the phone company's business records rather than a customer's private papers.

b. *Smith v. Maryland*

The Supreme Court's reasoning in *Smith v. Maryland*, 442 U.S. 735 (1979), also demonstrates that a customer has no reasonable expectation of privacy in cell-site information. In *Smith*, the telephone company installed a pen register at the request of the police to record numbers dialed from the defendant's telephone. The Supreme Court held both that telephone users had no subjective expectation of privacy in dialed telephone numbers and also that any such expectation is not one that society is prepared to recognize as reasonable. *See Smith*, 442 U.S. at 742-44. The Court's reasoning in *Smith* applies equally to cell-site records.

In *Smith*, regarding the customer's subjective expectation of privacy, the Court stated: "we doubt that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed." *Id.* at 742. Similarly, cell phone users understand that they must send a signal which is received by a cell phone company's antenna if the company is going to route their call to its intended recipient.

In *Smith*, the Supreme Court further held that even if the defendant had a subjective expectation of privacy in his dialed telephone numbers, "this expectation is not one that society is prepared to recognize as reasonable." *Id*. at 743 (internal quotation marks omitted). The Court explained that "[t]his Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties," and it held that the user "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business." *Id.* at 743-44. Here, a cell phone user voluntarily transmits a signal to a cell tower for his call to be connected, and the provider thereby creates records, for its own business purposes, regarding which of its cell towers it used to complete the call. If anything, the privacy interest in cell-site information is even less than the privacy interest in a dialed phone number: the location of the cell phone tower handling a customer's call is generated internally by the phone company and is not typically known by the customer. A customer's Fourth Amendment rights are not violated when the phone company reveals to the government its own internal records that were never in the possession or control of the customer.

The magistrate judge distinguished *Smith v. Maryland* by arguing that a customer has not "voluntarily conveyed" cell-site information to the service provider,

see Magistrate Opinion, 747 F. Supp. 2d at 843-44, but that argument is contradicted by the providers' terms of service and departs from the reasoning of *Smith*. Customers of MetroPCS and T-Mobile agree to contractual terms of service and privacy policies, and these agreements demonstrate that customers voluntarily convey location information to their providers. MetroPCS's privacy policy states:

> As an integral part of enabling wireless communications, information regarding the general location of your phone or wireless device is collected and used by the MetroPCS network. Your wireless device sends out periodic signals to the nearest radio tower/cell site providing information, including information regarding the location within the network, which allows the network to properly route an incoming call or message, and to provide the services that you may have subscribed to. This network location information derived from providing our Service, in addition to being covered by this Policy, is CPNI and is protected as described above.

See metropcs.com/metro/tac/termsAndConditions.jsp?terms=Privacy%20Policy (last visited February 14, 2012). Similarly, T-Mobile's privacy policy includes provisions stating that "[o]ur network detects your device's approximate location whenever it is turned on (subject to coverage limitations)," that "[t]his location technology makes the routing of wireless communications possible," and that "our systems capture details about the type and location of wireless device(s) you use." t-mobile.com/company/website/privacypolicy.aspx (last visited February 14, 2012).[4]

[4]The Third Circuit asserted that a customer did not voluntarily disclose location information because "it is unlikely that cell phone customers are aware that their cell phone providers *collect* and

It further informs customers that "[w]e may also use this technology to disclose, without a user's consent, the approximate location of a wireless device to a governmental entity or law enforcement authority when we are served with lawful process or reasonably believe there is an emergency involving risk of death or serious physical harm." *Id.* Because customers know that cell phone companies must obtain their location information in order to connect cell-phone calls, they voluntarily convey location information to cell phone companies under the principles of *Smith v. Maryland*, and the Fourth Amendment is not violated when that information is turned over to the government.

The magistrate judge's assertion that a customer does not voluntarily convey cell-site information to the service provider is based on an assumption that cell phone users are ignorant of cell phone technology, but that assumption departs from the reasoning of *Smith v. Maryland*. S*ee Magistrate Judge Opinion*, 747 F. Supp. 2d at

---

store historical location information." *In re Application of United States*, 620 F.3d at 317. These privacy policies demonstrate that customers are in fact informed that providers collect location information. The Supreme Court also rejected a similar argument in *Smith v. Maryland*, where it held that "[t]he fortuity of whether or not the phone company in fact elects to make a quasi-permanent record of a particular number dialed does not in our view, make any constitutional difference." *Smith*, 442 U.S. at 745. The Court explained that "[r]egardless of the phone company's election, petitioner voluntarily conveyed to it information that it had facilities for recording and that it was free to record." *Id.*; s*ee also United States v. Gallo*, 123 F.2d 229, 231 (2d Cir. 1941) (L. Hand, Swan, A. Hand, JJ.) ("When a person takes up a telephone he knows that the company will make, or may make, some kind of a record of the event, and he must be deemed to consent to whatever record the business conveniences of the company requires."); *In re Application of the United States*, ___ F. Supp. 2d ___, 2011 WL 3678934, at *8 (E.D.N.Y. Aug. 22, 2011) ("Public ignorance as to the existence of cell-site-location records, however, cannot long be maintained.")

844 (asserting that "a cell phone user may well have no reason to suspect that her location was exposed to anyone"). In contrast, the Supreme Court in *Smith v. Maryland* assumed that telephone users were familiar with telephone technology. *See Smith*, 442 U.S. at 742 ("All telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed. All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills."). As in *Smith*, when a court evaluates whether an expectation of privacy is objectively reasonable, this evaluation should be made based on a reasonable understanding of technology. The *Magistrate Judge Opinion*'s "assumption of ignorance" is therefore inconsistent with *Smith v. Maryland*.

In addition, users will know from their experience with cell phones that cell phones communicate with a provider's cell towers and that these communications will convey information to the provider about their location. Indeed, cell phone users routinely experience the frustration associated with dropped calls and recognize that calls are dropped when a phone's radio signal is having difficulty reaching a tower clearly. Cell phones usually display bars representing the strength of the signal between the phone and tower. Cell phone users understand that the provider will

know the location of its own cell towers and that the provider will thus have some knowledge of the user's location. *See In re Application of the United States*, ___ F. Supp. 2d ___, 2011 WL 3678934, at *8 (E.D.N.Y. Aug. 22, 2011) (stating that the assertion that cell-site information has not been voluntarily conveyed to the provider "relies too heavily on cell-phone users remaining unaware of the capacities of cellular technology, a doubtful proposition in the first place").[5]

[5]Furthermore, a 2703(d) order could be used to compel disclosure of historical cell-site records even if the *Magistrate Judge Opinion* were correct that a cell phone user does not voluntarily convey cell-site information to the telephone company. In general, a witness may testify to the extent of her personal knowledge, *see* Fed. R. Evid. 602, and the scope of her testimony regarding a defendant is not limited to matters the defendant voluntarily disclosed to her. Similarly, no inquiry into voluntariness is necessary when a business is compelled to disclose its own records made without governmental intervention. For example, if a store were to videotape a shoplifter using a hidden camera in its showroom, the government could subpoena the videotape without violating the shoplifter's Fourth Amendment rights, even though the shoplifter did not realize he was being recorded.

In *United States v. Miller*, 425 U.S. 435 (1976), in which the Supreme Court held that a customer had no privacy interest in his bank records, the Court addressed voluntariness for a reason not present in this case: the bank was required by the Bank Secrecy Act to keep the targeted records. The Supreme Court held that the mandatory record-keeping requirement of the Act did not create a Fourth Amendment interest in bank records "where none existed before" because the records contained "only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business." *Miller*, 425 U.S. at 441-42. In contrast to bank records, cell-site records are kept at the provider's discretion rather than at the direction of the government. An inquiry into voluntariness is called for only when the government has imposed upon the business a mandatory records retention requirement or is acting as a government agent in collecting and disclosing information prospectively, as in *Smith v. Maryland*. For example, the Supreme Court did not address voluntariness in *SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735 (1984), which held that the target of an investigation had no right to notice of subpoenas issued to third parties. *See id.* at 743 n. 11 ("It should be noted that any Fourth Amendment claims that might be asserted by respondents are substantially weaker than those of the bank customer in *Miller* because respondents, unlike the customer, cannot argue that the subpoena recipients were required by law to keep the records in question.").

c. *Other cases*

Courts have applied the principle that information revealed to a third party may be disclosed to the government in a wide variety of other contexts. The Supreme Court has applied this third-party principle to confidential statements made in the presence of an informant. *See Hoffa v. United States*, 385 U.S. 293, 302 (1966). The Court has applied it to financial and other records in the hands of third-party businesses. *See SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984); *see also Donaldson v. United States*, 400 U.S. 517, 522-23 (1971) (holding that taxpayer was not entitled to intervene in proceeding to enforce summons for his employment records and stating "what is sought here by the Internal Revenue Service . . . is the production of Acme's records and not the records of the taxpayer"). Appellate courts have applied this third-party principle to records of communications ranging from telephone billing records to ISP subscriber information to IP addresses of websites visited. *See Reporters Committee for Freedom of Press v. AT&T*, 593 F.2d 1030, 1043 (D.C. Cir. 1978) (rejecting Fourth Amendment challenge to subpoena for telephone records and explaining that when an individual transacts business with others, "he leaves behind, as evidence of his activity, the records and recollections of others. He cannot expect that these activities are his private affair."); *United States v. Perrine*, 518 F.3d 1196, 1204 (10th Cir. 2008) ("Every federal court to address this

issue has held that subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation."); *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008) (holding that email users have no reasonable expectation of privacy in to/from addresses of their messages or in IP addresses of websites visited). This Court also previously rejected a Fourth Amendment challenge to subpoenas directed to a telegraph company for the content of telegrams sent by specified customers. *See Newfield v. Ryan*, 91 F.2d 700, 703 (5th Cir. 1937). Under this third-party principle, users have no reasonable expectation of privacy in historical cell-site records.

Numerous district court cases have relied on *Smith* and *Miller* and rejected Fourth Amendment challenges to acquisition of historical cell-site records without a warrant. *See, e.g.*, *United States v. Dye*, 2011 WL 1595255, at *9 (N.D. Ohio April 27, 2011) (denying motion to suppress historical cell-site data); *United States v. Velasquez*, 2010 WL 4286276, at *5 (N.D. Cal. Oct. 22, 2010) (same); *United States v. Benford*, 2010 WL 1266507, at *3 (N.D. Ind. Mar. 26, 2010); *United States v. Suarez-Blanca*, 2008 WL 4200156, at *8-*11 (N.D. Ga. Mar. 26, 2008) (same); *Mitchell v. State*, 25 So.3d 632, 635 (Fla. Dist. Ct. App. 2009) (same). *But see In re Application of United States*, 620 F.3d at 313, 317 (asserting that location information is not voluntarily conveyed to a cell phone provider, but nevertheless stating that

historical cell-site records are "obtainable under a § 2703(d) order and that such an order does not require the traditional probable cause determination"); *In re Application of United States*, ___ F. Supp. 2d ___, 2011 WL 3678934 at *9-*11 (E.D.N.Y. Aug. 22, 2011) (holding that a warrant is required to compel disclosure of historical cell-site records).

2. As business records in the possession of a third party, cell-site records should not be judged under standards applicable to surreptitiously-installed tracking devices.

The *Magistrate Judge Opinion* analyzed the compelled disclosure of cell-site records under the standards used for tracking devices surreptitiously installed by the government, holding that "[c]ompelled warrantless disclosure of cell-site data violates the Fourth Amendment under the separate authorities of [*United States v. Karo*, 468 U.S. 705 (1984)] and [*United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010), *aff'd on other grounds sub nom. United States v. Jones*, ___ U.S. ___, 2012 WL 171117 (S. Ct. Jan. 23, 2012)]." *Magistrate Judge Opinion*, 747 F. Supp. 2d at 846. This is error: as business records in the possession of a third party, cell-site records should not be judged under standards applicable to surreptitiously-installed tracking devices.

In *Karo, United States v. Knotts*, 460 U.S. 276, 282 (1983), and now *United States v. Jones*, ___ U.S. ___, 2012 WL 171117 (S. Ct. Jan. 23, 2012), the Supreme Court has addressed the limited circumstances in which the Fourth Amendment

permits law enforcement to use a surreptitiously-installed beeper or GPS device to obtain location information on an ongoing basis without a warrant. The Supreme Court, however, has never applied the standards of these cases to business records cases, even though many kinds of business records may reveal someone's location at a particular time or other private facts. Instead, the Court's business records cases have been governed by the rule "that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities." *Miller*, 425 U.S. at 443.

For example, in *Karo*, a tracking-device decision, the Supreme Court held that police monitoring of a beeper that disclosed information about the interior of a private home required a warrant. *See Karo*, 468 U.S. at 715. A pen register on a traditional landline phone can reveal when phone calls are made from the interior of a private home. Yet the Court held in *Smith v. Maryland* that use of a pen register device does not require a warrant. *See Smith,* 442 U.S. at 745-46. It is thus apparent that the constitutional standards applicable to tracking devices do not apply when the government obtains information from a third party. Indeed, applying tracking-device standards to business records would have absurd and unworkable results. For example, if *Karo* were applied in this manner, the government would have to obtain a warrant, rather than a subpoena, to require a company to disclose phone records,

security surveillance videos, visitor sign-in sheets, or time-stamped photographs of an employee in her office, because any of these records could reveal someone's location in a private space at a particular time. Because compelled disclosure of business records is not governed by the standards applicable to surreptitiously-installed tracking devices, a 2703(d) order may be used to compel disclosure of historical cell-site records.

3. The Wireless Communication and Public Safety Act does not create a reasonable expectation of privacy in historical cell-site records.

The *Magistrate Judge Opinion* further errs in suggesting that a separate statute, the Wireless Communication and Public Safety Act of 1999 ("WCPSA"), Pub. L. No. 106-81, § 5, 113 Stat. 1286 (1999), is relevant to whether there is an expectation of privacy under the Fourth Amendment in historical cell-site information. *See Magistrate Judge Opinion*, 747 F. Supp. 2d at 841-43. Any argument that the WCPSA creates a Fourth Amendment privacy interest has now been foreclosed by the Supreme Court's recent rejection of the proposition that statutes can create a constitutional reasonable expectation of privacy. In *City of Ontario v. Quon*, 130 S. Ct. 2619 (2010), Quon argued that a violation of 18 U.S.C. § 2702 rendered a search of his text messages unreasonable under the Fourth Amendment. The Supreme Court rejected the notion that § 2702 created Fourth Amendment rights: "Respondents point

to no authority for the proposition that the existence of statutory protection renders a search *per se* unreasonable under the Fourth Amendment. And the precedents counsel otherwise." *Id.* at 2632 (citing *Virginia v. Moore*, 553 U.S. 164, 168 (2008), and *California v. Greenwood*, 486 U.S. 35, 43 (1988)). Similarly, in *United States v. Kington*, 801 F.2d 733, 737 (5th Cir. 1986), this Court held that the Right to Financial Privacy Act did not create Fourth Amendment rights and stated that "[t]he rights created by Congress are statutory, not constitutional."

In any case, the WCPSA allows compelled disclosure pursuant to a 2703(d) order. In particular, the WCPSA amended 47 U.S.C. § 222, which provides that "*[e]xcept as required by law* or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information" in certain specified situations. 47 U.S.C. § 222(c)(1) (emphasis added).[6] The phrase "except as required by law" encompasses appropriate criminal legal process. *See Parastino v. Conestoga Tel & Tel. Co.*, 1999 WL 636664, at *1-*2 (E.D.

[6]The WCPSA amended 47 U.S.C. § 222 to specify that a customer "shall not be considered to have approved the use or disclosure of or access to" call location information without "express prior authorization of the customer." WCPSA, Pub. L. No. 106-81, § 5, 113 Stat. 1286 (1999). Thus, it merely addressed the requirements for customer consent and did not create any new restrictions on access, use, or disclosure of customer location information.

Pa, Aug. 18, 1999) (holding that a valid subpoena falls within the "except as required by law" exception of § 222(c)(1)).

Because there is no actual conflict between § 2703(d) and the WCPSA, and given the "strong presumption of constitutionality" of federal statutes challenged on Fourth Amendment grounds, *United States v. Watson*, 423 U.S. 411, 416 (1976), there is no basis to conclude that Congress intended to render one of its statutes unconstitutional by enacting another. Moreover, 47 U.S.C. § 222(c)(1) protects not only cell phone location information; it protects all "individually identifiable customer propriety network information," which includes dialed phone numbers. Thus, the *Magistrate Judge Opinion*'s reasoning suggests that even use of a traditional telephone pen register could violate the Fourth Amendment, as dialed telephone numbers are also protected by § 222. This result is inconsistent with *Smith v. Maryland*, and it should be rejected.

B. Compulsory Process is Subject to a Reasonableness Standard, Not a Warrant Requirement.

The compelled disclosure of historical cell-site information in this case is supported not only by *Miller* and *Smith v. Maryland*, but also by the more general law applicable to subpoenas. The subpoena power is "the authority to command persons to appear and testify or to produce documents or things." *In re Subpoena Duces*

Tecum, 228 F.3d 341, 346 (4th Cir. 2000). A 2703(d) order functions as a judicial subpoena. It compels the recipient to produce specified information; the recipient may move to quash; and it remains at all times under the supervision of the issuing court. *See* 18 U.S.C. § 2703(d). Thus, cases addressing the Fourth Amendment principles applicable to subpoenas also apply to 2703(d) orders.[7] Under these cases, no warrant or showing of probable cause is required to use a subpoena to compel disclosure of non-privileged evidence relevant to a criminal investigation.

A 2703(d) order may be used to compel disclosure of historical cell-site records because the Fourth Amendment allows the United States to use a subpoena to compel disclosure of information relevant to a criminal investigation. By its terms, the Fourth Amendment protects people against unreasonable searches and seizures, but it imposes a probable-cause requirement only on the issuance of warrants. *See* U.S. Const. amend. IV ("and no Warrants shall issue, but upon probable cause"). The Supreme Court has explicitly rejected a probable-cause standard for subpoenas: "the

---

[7]The Supreme Court has explained the reason why the Fourth Amendment distinguishes the compulsion of subpoenas from other forms of forcible search and seizure, and this reasoning is equally applicable to 2703(d) orders:

> 'The latter is abrupt, is effected with force or the threat of it and often in demeaning circumstances, and, in the case of arrest, results in a record involving social stigma. A subpoena is served in the same manner as other legal process; it involves no stigma whatever; if the time for appearance is inconvenient, this can generally be altered; and it remains at all times under the control and supervision of a court.'

United States v. Dionisio, 410 U.S. 1, 10 (1973) (quoting *United States v. Doe*, 457 F.2d 895, 898 (2d Cir. 1972) (Friendly, J.)).

Government cannot be required to justify the issuance of a grand jury subpoena by presenting evidence sufficient to establish probable cause because the very purpose of requesting the information is to ascertain whether probable cause exists.*"* *United States v. R Enterprises, Inc.*, 498 U.S. 292, 297 (1991).

Instead of a probable cause standard, the Supreme Court has repeatedly held that under the Fourth Amendment, subpoenas must satisfy only a reasonableness standard. For example, in *Wilson v. United States*, 221 U.S. 361, 376 (1911), the Court held that "there is no unreasonable search and seizure when a [subpoena], suitably specific and properly limited in its scope, calls for the production of documents which, as against their lawful owner to whom the writ is directed, the party procuring its issuance is entitled to have produced." The Court affirmed this rule in *Oklahoma Press Publishing Co. v. Walling*, 327 U.S. 186, 208 (1946), when it held that "the Fourth [Amendment], if applicable [to a subpoena], at the most guards against abuse only by way of too much indefiniteness or breadth in the things required to be 'particularly described,' if also the inquiry is one the demanding agency is authorized by law to make and the materials specified are relevant. The gist of the protection is in the requirement, expressed in terms, that the disclosure sought shall not be unreasonable." *See also Donovan v. Lone Steer, Inc.*, 464 U.S. 408, 415 (1984); *In re Subpoena Duces Tecum*, 228 F.3d at 346-49 (discussing the Fourth

Amendment's reasonableness requirement for subpoenas). Because subpoenas are subject only to a reasonableness requirement, the district court erred in imposing a probable cause requirement for compelled disclosure of historical cell-site records.

The subpoena power is grounded in the long-standing principle that the government has the right to every witness's testimony. The Supreme Court has repeatedly confirmed that "'the public . . . has a right to every man's evidence,' except for those persons protected by a constitutional, common-law, or statutory privilege." *Branzburg v. Hayes*, 408 U.S. 665, 688 (1972).[8] The principle has remarkably deep roots. The Supreme Court has traced it to as early as 1562 and held that it "was considered an 'indubitable certainty' that 'cannot be denied' by 1742." *Kastigar v. United States*, 406 U.S. 441, 443 (1972) (citing Statute of Elizabeth, 5 Eliz. 1, c. 9, s. 12 (1562) and "parliamentary debate on the Bill to Indemnify Evidence, particularly the remarks of the Duke of Argyle and Lord Chancellor Hardwicke, reported in 12 T. Hansard, Parliamentary History of England 675, 693 (1812).").[9] Under this principle, the United States has the right to compel disclosure

[8]Although there are a few well-established privileges against compulsory process, such as the privilege against compulsory self-incrimination and the attorney-client privilege, the Supreme Court has recognized that "exceptions to the demand for every man's evidence are not lightly created nor expansively construed, for they are in derogation of the search for truth." *United States v. Nixon*, 418 U.S. 683, 710 (1974).

[9]The 1562 statute imposed a penalty of £10 plus damages on a person summoned to testify who failed to appear in court. *See Blair v. United States*, 250 U.S. 273, 279 (1919).

of the cell-site records of T-Mobile and MetroPCS because it has the right to every person's evidence and because the targeted cell-site records are evidence relevant and material to a criminal investigation.

The Supreme Court has also explained that the subpoena authority is essential to courts' ability to ascertain the truth: "[t]he need to develop all relevant facts in the adversary system is both fundamental and comprehensive. The ends of criminal justice would be defeated if judgments were to be founded on a partial or speculative presentation of the facts." *United States v. Nixon*, 418 U.S. 683, 709 (1974) (upholding subpoena to the President to produce certain tape recordings and documents). Thus, "[t]o ensure that justice is done, it is imperative to the function of courts that compulsory process be available for the production of evidence needed either by the prosecution or by the defense." *Id.* If courts were to reverse these rules and declare large categories of business records off limits to compulsory process, the search for truth through the judicial process would be substantially impaired. This Court should reject the district court's imposition of a warrant requirement for compelled disclosure of historical cell-site records.

C. Even Under the Standards Applicable to Surreptitiously Installed Tracking Devices, the Fourth Amendment Does Not Bar Compelled Disclosure of Cell-site Records.

As discussed in section I.A.2 above, cell-site records should not be judged under standards applicable to surreptitiously-installed tracking devices because they are business records in the possession of a third party. But even measured against the standards of the Supreme Court's tracking device cases, the United States does not violate the Fourth Amendment when it obtains historical cell-site information without a warrant.

This alternative argument depends on facts regarding the accuracy of historical cell-site information. If this Court finds it necessary to reach the question of the accuracy of historical cell-site records, remand to the district court for fact-finding will be necessary. As discussed in section II below, the magistrate judge's judicially-noticed findings must be rejected because they are subject to dispute and thus inappropriate for judicial notice. Before the district court, the United States submitted the MetroPCS affidavit stating that its cell-site records cannot locate a cell phone with precision, and the United States suggested a hearing to obtain similar testimony from T-Mobile. (A. 85, 109-12). The district court, however, did not hold a hearing or make factual findings regarding the accuracy of cell-site records. At a hearing, the United States would obtain testimony from T-Mobile or present

testimony from others familiar with the records of T-Mobile or MetroPCS. The United States believes that this evidence would demonstrate that the historical cell-site records sought by the United States would reveal only general location information about a cell phone (e.g. location within a region with average radius of a mile or more) and would not reveal the location of a cell phone with precision sufficient to reveal facts about the interior of a protected space. Under these facts, obtaining historical cell-site records without a warrant is consistent with the tracking-device standards of *United States v. Karo*, 468 U.S. 705 (1984), and *United States v. Jones*, ___ U.S. ___, 2012 WL 171117 (S. Ct. Jan. 23, 2012).

The Supreme Court has made clear that in certain limited circumstances, mere use of a tracking device, even when surreptitiously placed by the government, does not implicate Fourth Amendment privacy concerns. *See United States v. Knotts*, 460 U.S. 276, 282 (1983) (police monitoring of beeper signals along public roads did not invade any legitimate expectation of privacy). Subsequently, *Karo* and *Jones* have held that certain uses of tracking devices do implicate the Fourth Amendment, but obtaining historical cell-site records without a warrant is consistent with these decisions.

Under *United States v. Karo*, 468 U.S. 705 (1984), a warrant is required to use a surreptitiously-installed tracking device if the device reveals facts about the interior

of a constitutionally protected space. In *Karo*, agents installed a radio transmitter in a can of ether expected to be used in processing cocaine, and they monitored the signal from the beeper as it moved through a series of residences and multi-unit storage facilities. *See id*. at 708-09. Where the tracking system enabled the government to locate the can of ether in particular residences, the Supreme Court found that the Fourth Amendment had been infringed. *See id.* at 715. Importantly, the Court found no Fourth Amendment violation where the beeper disclosed only the general location of the ether, even though the ether was in a private space at the time the government obtained this general location information. In particular, agents tracked the transmitter to a multi-unit storage facility, then used their senses of smell to determine the particular unit containing the ether. *See id.* at 708. The Supreme Court concluded that this use of the transmitter did not violate the Fourth Amendment. *See id.* at 720. Thus, *Karo* holds only that government use of a tracking device violates the Fourth Amendment where the monitoring actually reveals the *particular* private location in which the tracked object may be found. Because cell-site records are not sufficiently precise to reveal a particular private location in which a cell phone may be found, cell-site records do not implicate the Fourth Amendment under *Karo*.

Jones, the Supreme Court's recent GPS-monitoring case, imposes additional limitations on the warrantless use of GPS monitoring by law enforcement, but obtaining historical cell-site records does not violate these restrictions either. In *Jones*, agents installed a GPS tracking device on the undercarriage of Jones's car and tracked its movements for 28 days. *See Jones*, 2012 WL 171117 at *2. Based on its determination that the agents had committed a common-law trespass, the Court held that "the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search.'" *Jones*, 2012 WL 171117 at *3. The United States does not violate this rule when it obtains historical cell-site data using a 2703(d) order, as such an order requires no installation, trespass, or physical intrusion by the government. More broadly, the Court in *Jones* looked to the original scope of Fourth Amendment protection and stated that the Fourth Amendment "must provide at a minimum the degree of protection it afforded when it was adopted." *Jones*, 2012 WL 171117 at *7. But as discussed in section I.B above, compulsory process was firmly established when the Fourth Amendment was adopted. *See Kastigar*, 406 U.S. at 443-44 (discussing history of compulsory process and stating that "[t]he first Congress recognized the testimonial duty in the Judiciary Act of 1789"). *Jones*'s originalist approach thus

supports allowing the United States to use a 2703(d) order to compel disclosure of historical cell-site records.

Nor does obtaining historical cell-site records via a 2703(d) violate Justice Alito's statement in his concurrence in *Jones* (joined by Justices Ginsburg, Breyer, and Kagan) that "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy." *See Jones*, 2012 WL 171117 at *17 (Alito, J., concurring).[10] First, by its terms, this statement applies to "monitoring." When the United States obtains historical cell-site records, it is not monitoring ongoing events: it is obtaining information concerning past events and previously collected by a third party acting independently of the government. Nothing in Justice Alito's concurrence limits the scope of information the United States may obtain from witnesses.

Second, cell-site records are less precise and less comprehensive than GPS-tracking information. They indicate only the general area of a cell phone when a call is made, and they may include no records for hours or days if no call is made. This lack of precision is significant. Justice Sotomayor expressed concern that GPS generates "a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and

[10] In a separate concurring opinion, Justice Sotomayor also explicitly endorsed this statement. *See Jones*, 2012 WL 171117 at *8 (Sotomayor, J., concurring).

sexual associations." *Jones*, 2012 WL 171117 at *9 (Sotomayor, J., concurring). Far from pinpointing the location of a car's every movement, cell-site records do not supply this kind of precise information regarding every place the cell phone user visited: they will not distinguish between a visit to a psychiatrist and a visit to the nearby mall or convenience store. Thus, the United States does not conduct a "search" under *Jones* when it uses a 2703(d) order to compel disclosure of historical cell-site records.

Justice Alito's concurrence in *Jones* also supports upholding the use of a 2703(d) order to compel disclosure of historical cell-site records. Justice Alito's concurrence favors deference to Congress to resolve privacy issues involving modern technology: "In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. . . . A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way." *Jones*, 2012 WL 171117 at *17 (Altio, J., concurring). With respect to records of cell phone providers, Congress has done just that: through the Stored Communications Act, 18 U.S.C. § 2701-2712, Congress enacted comprehensive legislation controlling government access to records of cell phone providers. Here, the United States complied with that Act in seeking a 2703(d) order and offering specific and articulable facts that the historical cell-site

records sought were relevant and material to an ongoing criminal investigations. The district court erred in holding that the Act violated the Fourth Amendment.

II. THE JUDICIALLY-NOTICED "FINDINGS OF FACT" ARE SUBJECT TO REASONABLE DISPUTE AND MUST BE REJECTED.

The magistrate judge abused his discretion in taking judicial notice under Rule 201 of the Federal Rules of Evidence of the structure of the phone companies' cellular networks, the location information generated by the phone companies, the accuracy of the location information generated by the phone companies, and the kind of location information stored and retained by service providers. *See Magistrate Judge Opinion*, 747 F. Supp. 2d at 831-35. These findings are subject to reasonable dispute under Rule 201 of the Federal Rules of Evidence.[11] It is unclear whether the district court adopted these findings of fact, but it overruled the United States's

[11] Although Rule 201 may not apply to an application for a 2703(d) order, *see* Rule 1101(d)(3) of the Federal Rules of Evidence, a court acting on an application for a 2703(d) order may not make factual findings not supported in the record before the court. In this respect, an application for a 2703(d) order is analogous to a suppression hearing: in a suppression hearing, the hearsay rule does not apply, but a court's factual findings must be supported by evidence in the record before the court. *Cf. United States v. Howard*, 106 F.3d 70, 73 (5th Cir. 1997) (appellate court reviews district court's findings of fact in suppression hearing for clear error, and finding of fact is clearly erroneous "when although there is evidence to support it, the reviewing court on the entire evidence is left with a firm and definite conviction that a mistake has been committed"). For example, in *United States v. Mariscal*, 285 F.3d 1127, 1131-32 (9th Cir. 2002), the district court's denial of a suppression motion was based on the district court's factual determination that a particular road "is a heavily traveled east-west street in the City of Phoenix." *Id.* at 1131. The Ninth Circuit rejected this finding of fact because it was not supported in the record before the court and because it was not suitable for judicial notice under Rule 201. *See id.* at 1131-32. *Mariscal* illustrates that the doctrine of judicial notice sets the appropriate limit on a court's authority to find facts beyond the scope of the record, even in a proceeding not strictly governed by the Federal Rules of Evidence.

objections to them, and it stated that the magistrate judge's ruling "subsists." (R. 43). This Court should reject the "findings of fact" in any case because they are not appropriate for judicial notice.[12]

Under Rule 201 of the Federal Rules of Evidence, "[a] judicially noticed fact must be one not subject to reasonable dispute in that it is either (1) generally known within the territorial jurisdiction of the trial court or (2) capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned." As the Advisory Committee Notes to Rule 201 caution, "[a] high degree of indisputability is the essential prerequisite." Advisory Committee Note to Subdivision (a). Indeed, "the tradition has been one of caution in requiring that the matter be beyond reasonable controversy." *Id.* at Note to Subdivision (b).

This Court has confirmed these stringent requirements for judicial notice: "judicial notice applies to self-evident truths that no reasonable person could

[12]To apply the standard for surreptitiously-installed tracking devices to cell-site records, a court needs facts about the precision of the records. The best mechanism to establish facts regarding the precision of cell-site records would be to review actual cell-site records produced in response to a 2703(d) order. In the context of a motion to suppress, a court could review the actual records produced by the provider, rather than trying to surmise how accurate the records produced by a provider might be. This approach would be most consistent with the principle that "[t]he constitutional validity of a warrantless search is pre-eminently the sort of question which can only be decided in the concrete factual context of the individual case." *Sibron v. New York*, 392 U.S. 40, 59 (1968). *See also United States v. Warshak*, 532 F.3d 521, 528 (6th Cir. 2008) (en banc) (stating that the reasonableness of Fourth Amendment searches are based on "case-by-case determinations that turn on the concrete, not the general, and offering incremental, not sweeping, pronouncements of law.").

question, truisms that approach platitudes or banalities." *Hardy v. Johns-Manville Sales Corp.*, 681 F.2d 334, 347 (5th Cir. 1982). *See, e.g., United States v. Henry*, 417 F.3d 493, 494 (5th Cir. 2005) ("We take judicial notice that both a 12-gauge shotgun and a 16-gauge shotgun have bore diameters in excess of one-half inch."). In *Hardy*, the Fifth Circuit held that the district court erred in taking judicial notice of the proposition that asbestos causes cancer. The court explained that "[t]he proposition that asbestos causes cancer, because it is inextricably linked to a host of disputed issues . . . is not at present so self-evident a proposition as to be subject to judicial notice." *Hardy*, 681 F.2d at 347-48. The court concluded that "[t]he rule of judicial notice 'contemplates there is to be no evidence before the jury in disproof.' . . . Surely where there is evidence on both sides of an issue the matter is subject to reasonable dispute." *Id.* at 348. *See also Taylor v. Charter Medical Corp.*, 162 F.3d 827, 830 (5th Cir. 1998) (proposition that a particular hospital was a state actor "was not the type of self-evident truth that no reasonable person could question, a truism that approaches platitude or banality, as required to be eligible for judicial notice under Rule 201" (internal quotation marks and brackets omitted)). The *Magistrate Judge Opinion*'s findings do not satisfy this standard.

Of the fifty paragraphs of the magistrate judge's "findings of fact," only the first, which states that cellular phones use radio waves to communicate with the

telephone network, is clearly appropriate for judicial notice under Rule 201. The *Magistrate Judge Opinion* relies primarily on congressional testimony of Matt Blaze, an Associate Professor of Computer and Information Science at the University of Pennsylvania. *See Magistrate Judge Opinion*, 747 F. Supp. 2d at 831-35 (citing Blaze's testimony in footnotes 13-17, 19, 21-35, 37-40, 42-46, and 51-55).[13] This testimony, which addresses both the structure of provider networks and their internal record keeping practices, addresses matters far from platitudes, banalities, or self-evident truths.

The United States believes that the magistrate judge's "findings of fact" are fundamentally inaccurate, but in any case, they are certainly subject to reasonable dispute. The "findings of fact" are contradicted by the sworn affidavit of MetroPCS. This affidavit indicates that the average MetroPCS "towers have a coverage radius of about one to two miles," that the radius is "no smaller than 100 yards in some densely populated urban areas," that MetroPCS "do[es] not currently create and store

[13]On June 24, 2010, Magistrate Judge Smith and Professor Blaze testified on the same panel before a congressional committee regarding the Electronic Communications Privacy Act. *See ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 12-31, 76-94 (2010). Essentially, Magistrate Judge Smith adopted Professor Blaze's out-of-court testimony as indisputable fact. This adoption violates the principle that "[j]udicial notice is denied to disputable propositions found in testimony at government hearings." 1 Jack B. Weinstein & Margaret A. Berger, *Weinstein's Federal Evidence* § 201.13[1][c] (McLaughlin ed., 2d ed. 2010).

cell-site information unless a call is made, " that MetroPCS stores only a record of the tower the phone was connected to at the beginning and end of the call, and that MetroPCS does not store cell-site records when a phone is idle. (A. 110-12). These statements of MetroPCS conflict with the assertions in the "findings of fact" that "a provider can pinpoint the phone's latitude and longitude to an accuracy within 50 meters or less," that carriers create records "that include the most accurate location information available to them," that "[s]ome carriers also store frequently updated, highly precise, location information not just when calls are made or received, but as the device moves around the network," that "[t]his data is sufficient to plot the target's movements hour by hour for the duration of the 60 day period covered by the government's request," and that "call detail records can now include the user's latitude and longitude." *Magistrate Judge Opinion*, 747 F. Supp. 2d at 833-35 (¶¶ 27, 31, 33, 49). Thus, the "findings of fact" are subject to reasonable dispute.

The "findings of fact" are also inconsistent with other court decisions and findings of the FCC. *See, e.g.*, *In re Applications of United States*, 509 F. Supp. 2d 76, 78 n.3 (D. Mass. 2007) ("In urban areas, cell towers can be only hundreds of feet apart. In rural areas, towers are often ten miles or more apart."); *In re Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems*, 15 FCC Rcd. 17442, 17462 (Sept. 8, 2000) (finding that a certain location-

finding technique accurate to within 500-1000 meters "would be significantly more precise" than "the location of the cell site or sector receiving the call."). Given the differences between the *Magistrate Judge Opinion*'s "findings of fact" and the findings of other courts, the FCC, and the sworn affidavit from MetroPCS, the "findings of fact" are subject to reasonable dispute and therefore not appropriate for judicial notice.[14]

CONCLUSION

Because historical cell-site records are business records of the cell phone providers to whom the 2703(d) orders are directed, this Court should reverse the district court's order and remand with instructions to grant the government's applications. Because the magistrate judge incorrectly took judicial notice of disputed facts, contrary to Fed. R. Evid. 201, this Court should vacate those findings;

[14]Procedurally, the magistrate judge also failed to provide the United States with adequate prior notice of the judicially-noticed facts. Under Rule 201(e), "[a] party is entitled upon timely request to an opportunity to be heard as to the propriety of taking judicial notice and the tenor of the matter noticed." *See also United States v. Garcia*, 672 F.2d 1349, 1356 n. 9 (11th Cir. 1982) ("Ordinarily, when a judge takes judicial notice of a fact other than at the request of a party (i.e., 'discretionary judicial notice'), he should notify the parties that he is doing so and afford them an opportunity to be heard."). Prior to issuing the *Magistrate Judge Opinion*, the magistrate judge did not inform the United States of the specific facts of which he intended to take judicial notice. Instead, the court only informed the United States of the broad categories from which he intended to draw facts. (A. 53-54). The United States objected that it could not "determine from the broad categories cited by the Court whether it is appropriate to take judicial notice of any particular facts that might fall within those categories." (A. 77). By providing the United States with notice only of broad categories, rather than specific facts, the magistrate judge did not provide the United States with a reasonable opportunity to respond to the judicially-noticed facts.

and if this Court finds it necessary to apply tracking-device standards to cell-site records, it should remand to the district court for factual findings regarding the accuracy of historical cell-site records.

Respectfully submitted,

KENNETH MAGIDSON
United States Attorney

RENATA A. GOWIE
Chief, Appellate Division

s/NATHAN JUDISH
NATHAN JUDISH
Senior Counsel
Computer Crime and Intellectual Property Section
United States Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530
(202) 616-7203
nathan.judish@usdoj.gov

CERTIFICATE OF SERVICE

I, Nathan Judish, hereby certify that on February 15, 2012, an electronic copy of the foregoing Brief for the United States was served by notice of electronic filing via this Court's ECF system upon all counsel of record. Upon notification that the electronically filed brief has been accepted as sufficient, and upon the Clerk's request, a paper copy of this brief will be placed in the United States Mail, postage prepaid, addressed to the Clerk.

s/Nathan Judish
NATHAN JUDISH
Senior Counsel

CERTIFICATE OF COMPLIANCE

1. This brief does comply with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because:

   this brief contains **11,742** words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5)and the type style requirements of Fed. R. App. P. 32(a)(6) because:

   this brief has been prepared in a proportionally spaced typeface using Corel WordPerfect X3 in Times New Roman, 14 point font for text and 12 point font for footnotes.

3. This brief complies with the privacy redaction requirement of 5th Cir. R. 25.2.13 because:

   this brief has been redacted of any personal data identifiers; the Appendix to this brief is being filed under seal.

4. This brief complies with the electronic submission of 5th Cir. R. 25.2.1, because:

   this is brief is an exact copy of the paper document.

5. This brief is free of viruses because:

   this brief has been scanned for viruses with the most recent version of Trend Micro scanning program.

s/Nathan Judish
NATHAN JUDISH
Senior Counsel