APPENDIX A

In the

United States Court of Appeals

For the Seventh Circuit

No. 17-2593

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

JUAN MANUEL SANCHEZ-JARA,

Defendant-Appellant.

Appeal from the United States District Court for the
Northern District of Illinois, Eastern Division.
No. 15 CR 457 — **Jorge L. Alonso**, *Judge*.

ARGUED APRIL 6, 2018 — DECIDED MAY 3, 2018

Before EASTERBROOK, RIPPLE, and HAMILTON, *Circuit Judges*.

EASTERBROOK, *Circuit Judge*. Like *United States v. Patrick*, 842 F.3d 540 (7th Cir. 2016), this appeal concerns the use of a cell-site simulator to locate someone. And like *Patrick* it does not require us to determine when, if ever, the use of this device must be authorized by a warrant supported by probable cause, for in this case such a warrant was obtained.

The warrant, issued by a federal district judge in July 2015, authorizes federal agents to use pen registers, trap-and-trace devices, historical cell-call records, and "electronic investigative techniques … to capture and analyze signals emitted by the **Subject Phones**, including in response to signals sent by law enforcement officers" (boldface in original) to find two cell phones and understand the nature of their owners' apparently criminal activity. The warrant's reference to "electronic investigative techniques" is a description of a cell-site simulator, a device that pretends to be a cell tower and harvests identifying information, including location data, about every phone that responds to its signals. The Department of Justice contends that it discards information about all phones other than those it has been programmed to look for and does not obtain the contents of any call. Here is the Department's description:

> Cell-site simulators … function by transmitting as a cell tower. In response to the signals emitted by the simulator, cellular devices in the proximity of the device identify the simulator as the most attractive cell tower in the area and thus transmit signals to the simulator that identify the device in the same way that they would with a networked tower.
>
> A cell-site simulator receives and uses an industry standard unique identifying number assigned by a device manufacturer or cellular network provider. When used to locate a known cellular device, a cell-site simulator initially receives the unique identifying number from multiple devices in the vicinity of the simulator. Once the cell-site simulator identifies the specific cellular device for which it is looking, it will obtain the signaling information relating only to that particular phone. When used to identify an unknown device, the cell-site simulator obtains signaling information from non-target devices in the target's vicinity for the limited purpose of distinguishing the target device.

> By transmitting as a cell tower, cell-site simulators acquire the identifying information from cellular devices. This identifying information is limited, however. Cell-site simulators provide only the relative signal strength and general direction of a subject cellular telephone; they do not function as a GPS locator, as they do not obtain or download any location information from the device or its applications. Moreover, cell-site simulators used by the Department must be configured as pen registers, and may not be used to collect the contents of any communication, in accordance with 18 U.S.C. §3127(3). This includes any data contained on the phone itself: the simulator does not remotely capture emails, texts, contact lists, images or any other data from the phone. In addition, Department cell-site simulators do not provide subscriber account information (for example, an account holder's name, address, or telephone number).

Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology (Sept. 3, 2015) at 2. See also the Wikipedia entry at <en.wikipedia.org/wiki/IMSI-catcher>.

Whether the simulator works this way is potentially important, because the warrant did not authorize the investigators to obtain the contents of any calls, to plumb any phone's address book or instant messages, or otherwise to get anything except location and certain metadata, the sorts of things available from pen registers and trap-and-trace devices. To get the contents of calls and messages, the agents would have needed a warrant under the wiretap statutes. 18 U.S.C. §§ 2510–22. The agents did not obtain a warrant of that kind or satisfy the conditions, such as the attempted use of other investigatory means and the minimization of intrusion, that are essential to wiretap warrants.

The warrant issued in 2015 was based not on the wiretap statutes but on 18 U.S.C. §2703(d) and Fed. R. Crim. P. 41. Subsection (d) provides that "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" permit a judge to issue a warrant for the production of information described in subsection (c), which includes cell-phone information such as numbers called, but not the content of conversations. (Subsections (a) and (b), which deal with stored communications such as email, are not at issue here.) Sanchez-Jara contends that "reasonable grounds" differs from "probable cause" and that a warrant issued under §2703(d) therefore does not comply with the Fourth Amendment, which provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

To this the United States replies that "reasonable grounds" is just an alternative way to describe probable cause, which under *Illinois v. Gates*, 462 U.S. 213 (1983), means enough to lead a prudent person to think that the search may well reveal evidence of crime. The prosecution also contends that, if there is a difference, something less than probable cause suffices to obtain the sort of information covered by §2703(c), much of which may be available without either probable cause or a warrant. (What kinds of cell-phone data require warrants is an issue in *Carpenter v. United States*, No. 16–402, which has been under advisement in the Supreme Court since November 29, 2017.)

None of this matters, however, because the warrant not only recites the language of §2703(d) but also states that the searches are justified by probable cause. The warrant declares that this finding applies to both §2703 and Rule 41, the

standard source of authority for criminal search and arrest warrants. Given the district judge's finding of probable cause—a finding that carries a strong presumption of correctness, see *United States v. McIntire*, 516 F.3d 576 (7th Cir. 2008)—this warrant suffices to support use of a cell-site simulator that does not gather information that would require a wiretap warrant. And because this warrant was supported by probable cause, the discoveries do not taint the later consents that enabled the agents to find 99 kilograms of cocaine and three guns.

Nothing in the record of this case suggests that the agents acquired information that would have required a wiretap warrant. Certainly the United States did not propose to use any information about the content of Sanchez-Jara's calls or personal data scraped from his cell phone. After the district court denied Sanchez-Jara's motion to suppress the location and traffic data, he entered a conditional guilty plea to drug and firearms charges and reserved the right to argue that the search was not supported by a valid warrant. We do not read either his conditional plea or his appellate brief as attempting to present a contention that the agents obtained or used information that would have required a wiretap warrant.

At oral argument counsel for Sanchez-Jara maintained that the warrant authorized a general search. Counsel seems to have meant two things by this: first that agents sought not contraband but evidence of crime, and second that the agents could follow the phones wherever they went. Neither of these is constitutionally problematic. The first theme harks back to the days before *Warden v. Hayden*, 387 U.S. 294 (1967), disapproved the "mere evidence" doctrine. *Hayden*

holds that searches for "mere evidence" do not violate the Fourth Amendment. The second theme misunderstands what makes a general warrant invalid. The Constitution demands that a warrant "particularly describ[e] the place to be searched, and the persons or things to be seized." Thus authorization to search a whole home for evidence of any crime flunks the particularity requirement. See *Andresen v. Maryland*, 427 U.S. 463, 480–82 (1976). But a warrant authorizing police to follow an identified phone, to see where it goes and what numbers it calls, particularly describes the evidence to be acquired. It is no different in principle from a warrant authorizing a GPS device that enables police to track the location of a moving car, and none of the Justices in *United States v. Jones*, 565 U.S. 400 (2012), saw any problem with such a warrant. The 2015 warrant is not an open-ended authorization for public officials to rummage where they please in order to see what turns up.

AFFIRMED

APPENDIX B

United States Court of Appeals

For the Seventh Circuit
Chicago, Illinois 60604

June 1, 2018

Before

FRANK H. EASTERBROOK, *Circuit Judge*

KENNETH F. RIPPLE, *Circuit Judge*

DAVID F. HAMILTON, *Circuit Judge*

No. 17-2593

UNITED STATES OF AMERICA,
Plaintiff-Appellee,

v.

JUAN MANUEL SANCHEZ-JARA,
Defendant-Appellant.

Appeal from the United States District Court for the Northern District of Illinois, Eastern Division.

No. 15 CR 457
Jorge L. Alonso, *Judge.*

Order

Defendant-appellant filed a petition for rehearing on May 11, 2018. All of the judges on the panel have voted to deny rehearing. The petition for rehearing is therefore DENIED.

UNITED STATES COURT OF APPEALS FOR THE SEVENTH CIRCUIT

Everett McKinley Dirksen United States Courthouse
Room 2722 - 219 S. Dearborn Street
Chicago, Illinois 60604

Office of the Clerk
Phone: (312) 435-5850
www.ca7.uscourts.gov

NOTICE OF ISSUANCE OF MANDATE

June 11, 2018

To: Thomas G. Bruton
UNITED STATES DISTRICT COURT
Northern District of Illinois
Chicago , IL 60604-0000

No. 17-2593	UNITED STATES OF AMERICA, Plaintiff - Appellee v. JUAN MANUEL SANCHEZ-JARA, Defendant - Appellant

Originating Case Information:

District Court No: 1:15-cr-00457-1
Northern District of Illinois, Eastern Division
District Judge Jorge L. Alonso

Herewith is the mandate of this court in this appeal, along with the Bill of Costs, if any. A certified copy of the opinion/order of the court and judgment, if any, and any direction as to costs shall constitute the mandate.

RECORD ON APPEAL STATUS: No record to be returned

NOTE TO COUNSEL:
If any physical and large documentary exhibits have been filed in the above-entitled cause, they are

to be withdrawn ten (10) days from the date of this notice. Exhibits not withdrawn during this period will be disposed of.

Please acknowledge receipt of these documents on the enclosed copy of this notice.

Received above mandate and record, if any, from the Clerk, U.S. Court of Appeals for the Seventh Circuit.

Date: **Received by:**

_____ _____

form name: **c7_Mandate**(form ID: **135**)

APPENDIX C

2984; Pub. L. 107–56, title II, § 212(a)(1), Oct. 26, 2001, 115 Stat. 284; Pub. L. 107–296, title II, § 225(d)(1), Nov. 25, 2002, 116 Stat. 2157; Pub. L. 108–21, title V, § 508(b), Apr. 30, 2003, 117 Stat. 684; Pub. L. 109–177, title I, § 107(a), (b)(1), (c), Mar. 9, 2006, 120 Stat. 202, 203; Pub. L. 110–401, title V, § 501(b)(2), Oct. 13, 2008, 122 Stat. 4251.)

AMENDMENTS

2008—Subsecs. (b)(6), (c)(5). Pub. L. 110–401 substituted "section 2258A" for "section 227 of the Victims of Child Abuse Act of 1990 (42 U.S.C. 13032)".

2006—Subsec. (a). Pub. L. 109–177, § 107(c), inserted "or (c)" after "Except as provided in subsection (b)".

Subsec. (b)(8). Pub. L. 109–177, § 107(b)(1)(A), struck out "Federal, State, or local" before "governmental entity".

Subsec. (c)(4). Pub. L. 109–177, § 107(b)(1)(B), added par. (4) and struck out former par. (4) which read as follows: "to a governmental entity, if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information;".

Subsec. (d). Pub. L. 109–177, § 107(a), added subsec. (d).

2003—Subsec. (b)(5). Pub. L. 108–21, § 508(b)(1)(C), which directed amendment of par. (5) by striking "or" at the end, could not be executed because "or" did not appear at the end. See 2002 Amendment note below.

Subsec. (b)(6). Pub. L. 108–21, § 508(b)(1)(D), added par. (6). Former par. (6) redesignated (7).

Subsec. (b)(6)(B). Pub. L. 108–21, § 508(b)(1)(A), struck out subpar. (B) which read as follows: "if required by section 227 of the Crime Control Act of 1990; or".

Subsec. (b)(7), (8). Pub. L. 108–21, § 508(b)(1)(B), redesignated pars. (6) and (7) as (7) and (8), respectively.

Subsec. (c)(5), (6). Pub. L. 108–21, § 508(b)(2), added par. (5) and redesignated former par. (5) as (6).

2002—Subsec. (b)(5). Pub. L. 107–296, § 225(d)(1)(A), struck out "or" at end.

Subsec. (b)(6)(A). Pub. L. 107–296, § 225(d)(1)(B), inserted "or" at end.

Subsec. (b)(6)(C). Pub. L. 107–296, § 225(d)(1)(C), struck out subpar. (C) which read as follows: "if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information without delay."

Subsec. (b)(7). Pub. L. 107–296, § 225(d)(1)(D), added par. (7).

2001—Pub. L. 107–56, § 212(a)(1)(A), substituted "Voluntary disclosure of customer communications or records" for "Disclosure of contents" in section catchline.

Subsec. (a)(3). Pub. L. 107–56, § 212(a)(1)(B), added par. (3).

Subsec. (b). Pub. L. 107–56, § 212(a)(1)(C), substituted "Exceptions for disclosure of communications" for "Exceptions" in heading and "A provider described in subsection (a)" for "A person or entity" in introductory provisions.

Subsec. (b)(6)(C). Pub. L. 107–56, § 212(a)(1)(D), added subpar. (C).

Subsec. (c). Pub. L. 107–56, § 212(a)(1)(E), added subsec. (c).

1998—Subsec. (b)(6). Pub. L. 105–314 amended par. (6) generally. Prior to amendment, par. (6) read as follows: "to a law enforcement agency, if such contents—

"(A) were inadvertently obtained by the service provider; and

"(B) appear to pertain to the commission of a crime."

1988—Subsec. (b)(2). Pub. L. 100–690 substituted "2517" for "2516".

EFFECTIVE DATE OF 2002 AMENDMENT

Amendment by Pub. L. 107–296 effective 60 days after Nov. 25, 2002, see section 4 of Pub. L. 107–296, set out as an Effective Date note under section 101 of Title 6, Domestic Security.

§ 2703. Required disclosure of customer communications or records

(a) CONTENTS OF WIRE OR ELECTRONIC COMMUNICATIONS IN ELECTRONIC STORAGE.—A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

(b) CONTENTS OF WIRE OR ELECTRONIC COMMUNICATIONS IN A REMOTE COMPUTING SERVICE.—(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.

(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service—

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

(c) RECORDS CONCERNING ELECTRONIC COMMUNICATION SERVICE OR REMOTE COMPUTING SERVICE.—(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to

or customer of such service (not including the contents of communications) only when the governmental entity—

(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction;

(B) obtains a court order for such disclosure under subsection (d) of this section;

(C) has the consent of the subscriber or customer to such disclosure;

(D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or

(E) seeks information under paragraph (2).

(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the—

(A) name;

(B) address;

(C) local and long distance telephone connection records, or records of session times and durations;

(D) length of service (including start date) and types of service utilized;

(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

(F) means and source of payment for such service (including any credit card or bank account number),

of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

(3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

(d) REQUIREMENTS FOR COURT ORDER.—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. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

(e) NO CAUSE OF ACTION AGAINST A PROVIDER DISCLOSING INFORMATION UNDER THIS CHAPTER.—No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter.

(f) REQUIREMENT TO PRESERVE EVIDENCE.—

(1) IN GENERAL.—A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

(2) PERIOD OF RETENTION.—Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.

(g) PRESENCE OF OFFICER NOT REQUIRED.—Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service.

(Added Pub. L. 99–508, title II, § 201[(a)], Oct. 21, 1986, 100 Stat. 1861; amended Pub. L. 100–690, title VII, §§ 7038, 7039, Nov. 18, 1988, 102 Stat. 4399; Pub. L. 103–322, title XXXIII, § 330003(b), Sept. 13, 1994, 108 Stat. 2140; Pub. L. 103–414, title II, § 207(a), Oct. 25, 1994, 108 Stat. 4292; Pub. L. 104–132, title VIII, § 804, Apr. 24, 1996, 110 Stat. 1305; Pub. L. 104–293, title VI, § 601(b), Oct. 11, 1996, 110 Stat. 3469; Pub. L. 104–294, title VI, § 605(f), Oct. 11, 1996, 110 Stat. 3510; Pub. L. 105–184, § 8, June 23, 1998, 112 Stat. 522; Pub. L. 107–56, title II, §§ 209(2), 210, 212(b)(1), 220(a)(1), (b), Oct. 26, 2001, 115 Stat. 283, 285, 291, 292; Pub. L. 107–273, div. B, title IV, § 4005(a)(2), div. C, title I, § 11010, Nov. 2, 2002, 116 Stat. 1812, 1822; Pub. L. 107–296, title II, § 225(h)(1), Nov. 25, 2002, 116 Stat. 2158; Pub. L. 109–162, title XI, § 1171(a)(1), Jan. 5, 2006, 119 Stat. 3123; Pub. L. 111–79, § 2(1), Oct. 19, 2009, 123 Stat. 2086.)

REFERENCES IN TEXT

The Federal Rules of Criminal Procedure, referred to in subsecs. (a), (b)(1)(A), and (c)(1)(B)(i), are set out in the Appendix to this title.

AMENDMENTS

2009—Subsecs. (a), (b)(1)(A), (c)(1)(A). Pub. L. 111–79, which directed substitution of "(or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction" for "by a court with jurisdiction over the offense under investigation or an equivalent State warrant", was executed by making the substitution for "by a court with jurisdiction over the offense under investigation or equivalent State warrant" to reflect the probable intent of Congress.

2006—Subsec. (c)(1)(C). Pub. L. 109–162 struck out "or" at end.

2002—Subsec. (c)(1)(E). Pub. L. 107–273, § 4005(a)(2), realigned margins.

Subsec. (e). Pub. L. 107–296 inserted ", statutory authorization" after "subpoena".

Subsec. (g). Pub. L. 107–273, § 11010, added subsec. (g).

2001—Pub. L. 107–56, § 212(b)(1)(A), substituted "Required disclosure of customer communications or

records'' for ''Requirements for governmental access'' in section catchline.

Subsec. (a). Pub. L. 107–56, §§ 209(2)(A), (B), 220(a)(1), substituted ''Contents of Wire or Electronic'' for ''Contents of Electronic'' in heading and ''contents of a wire or electronic'' for ''contents of an electronic'' in two places and ''using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation'' for ''under the Federal Rules of Criminal Procedure'' in text.

Subsec. (b). Pub. L. 107–56, § 209(2)(A), substituted ''Contents of Wire or Electronic'' for ''Contents of Electronic'' in heading.

Subsec. (b)(1). Pub. L. 107–56, §§ 209(2)(C), 220(a)(1), substituted ''any wire or electronic communication'' for ''any electronic communication'' in introductory provisions and ''using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation'' for ''under the Federal Rules of Criminal Procedure'' in subpar. (A).

Subsec. (b)(2). Pub. L. 107–56, § 209(2)(C), substituted ''any wire or electronic communication'' for ''any electronic communication'' in introductory provisions.

Subsec. (c)(1). Pub. L. 107–56, §§ 212(b)(1)(C), 220(a)(1), designated subpar. (A) and introductory provisions of subpar. (B) as par. (1), substituted ''A governmental entity may require a provider of electronic communication service or remote computing service to'' for ''(A) Except as provided in subparagraph (B), a provider of electronic communication service or remote computing service may'' and a closing parenthesis for provisions which began with ''covered by subsection (a) or (b) of this section) to any person other than a governmental entity.'' in former subpar. (A) and ended with ''(B) A provider of electronic communication service or remote computing service shall disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a) or (b) of this section) to a governmental entity'', redesignated clauses (i) to (iv) of former subpar. (B) as subpars. (A) to (D), respectively, substituted ''using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation'' for ''under the Federal Rules of Criminal Procedure'' in subpar. (A) and ''; or'' for period at end of subpar. (D), added subpar. (E), and redesignated former subpar. (C) as par. (2).

Subsec. (c)(2). Pub. L. 107–56, § 210, amended par. (2), as redesignated by section 212 of Pub. L. 107–56, by substituting ''entity the—'' for ''entity the name, address, local and long distance telephone toll billing records, telephone number or other subscriber number or identity, and length of service of a subscriber'' in introductory provisions, inserting subpars. (A) to (F), striking out ''and the types of services the subscriber or customer utilized,'' before ''when the governmental entity uses an administrative subpoena'', inserting ''of a subscriber'' at beginning of concluding provisions and designating ''to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).'' as remainder of concluding provisions.

Pub. L. 107–56, § 212(b)(1)(C)(iii), (D), redesignated subpar. (C) of par. (1) as par. (2) and temporarily substituted ''paragraph (1)'' for ''subparagraph (B)''.

Pub. L. 107–56, § 212(b)(1)(B), redesignated par. (2) as (3).

Subsec. (c)(3). Pub. L. 107–56, § 212(b)(1)(B), redesignated par. (2) as (3).

Subsec. (d). Pub. L. 107–56, § 220(b), struck out ''described in section 3127(2)(A)'' after ''court of competent jurisdiction''.

1998—Subsec. (c)(1)(B)(iv). Pub. L. 105–184 added cl. (iv).

1996—Subsec. (c)(1)(C). Pub. L. 104–293 inserted ''local and long distance'' after ''address,''.

Subsec. (d). Pub. L. 104–294 substituted ''in section 3127(2)(A)'' for ''in section 3126(2)(A)''.

Subsec. (f). Pub. L. 104–132 added subsec. (f).

1994—Subsec. (c)(1)(B). Pub. L. 103–414, § 207(a)(1)(A), redesignated cls. (ii) to (iv) as (i) to (iii), respectively, and struck out former cl. (i) which read as follows: ''uses an administrative subpoena authorized by a Federal or State statute, or a Federal or State grand jury or trial subpoena;''.

Subsec. (c)(1)(C). Pub. L. 103–414, § 207(a)(1)(B), added subpar. (C).

Subsec. (d). Pub. L. 103–414, § 207(a)(2), amended first sentence generally. Prior to amendment, first sentence read as follows: ''A court order for disclosure under subsection (b) or (c) of this section may be issued by any court that is a court of competent jurisdiction set forth in section 3127(2)(A) of this title and shall issue only if the governmental entity shows that there is reason to believe the contents of a wire or electronic communication, or the records or other information sought, are relevant to a legitimate law enforcement inquiry.''

Pub. L. 103–322 substituted ''section 3127(2)(A)'' for ''section 3126(2)(A)''.

1988—Subsecs. (b)(1)(B)(i), (c)(1)(B)(i). Pub. L. 100–690, § 7038, inserted ''or trial'' after ''grand jury''.

Subsec. (d). Pub. L. 100–690, § 7039, inserted ''may be issued by any court that is a court of competent jurisdiction set forth in section 3126(2)(A) of this title and'' before ''shall issue''.

EFFECTIVE DATE OF 2002 AMENDMENT

Amendment by Pub. L. 107–296 effective 60 days after Nov. 25, 2002, see section 4 of Pub. L. 107–296, set out as an Effective Date note under section 101 of Title 6, Domestic Security.

§ 2704. Backup preservation

(a) BACKUP PRESERVATION.—(1) A governmental entity acting under section 2703(b)(2) may include in its subpoena or court order a requirement that the service provider to whom the request is directed create a backup copy of the contents of the electronic communications sought in order to preserve those communications. Without notifying the subscriber or customer of such subpoena or court order, such service provider shall create such backup copy as soon as practicable consistent with its regular business practices and shall confirm to the governmental entity that such backup copy has been made. Such backup copy shall be created within two business days after receipt by the service provider of the subpoena or court order.

(2) Notice to the subscriber or customer shall be made by the governmental entity within three days after receipt of such confirmation, unless such notice is delayed pursuant to section 2705(a).

(3) The service provider shall not destroy such backup copy until the later of—

(A) the delivery of the information; or

(B) the resolution of any proceedings (including appeals of any proceeding) concerning the government's subpoena or court order.

(4) The service provider shall release such backup copy to the requesting governmental entity no sooner than fourteen days after the governmental entity's notice to the subscriber or customer if such service provider—

(A) has not received notice from the subscriber or customer that the subscriber or customer has challenged the governmental entity's request; and

APPENDIX D

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER RELATING TO TELEPHONE NUMBER (312) 399-9606 ("**SUBJECT PHONE 14**") AND TELEPHONE NUMBER (708) 261-2832 ("**SUBJECT PHONE 15**")

UNDER SEAL
No. 14 GJ 1008

Rubén Castillo
Chief Judge

WARRANT AND ORDER

THIS MATTER has come before the Court pursuant to an application by Paul H. Tzur, an attorney for the government, which application relates to:

a. the telephone currently assigned telephone number (312) 399-9606, and used by an unidentified individual ("UI5"), with service provided by Sprint/Nextel (hereafter, "**Subject Phone 14**"); and

b. the telephone currently assigned telephone number (708) 261-2832, and used by an unidentified individual ("UI6"), with service provided by Sprint/Nextel (hereafter, "**Subject Phone 15**") (collectively, the "**Subject Phones**").

In its Application, the government requests that this Court enter an order granting the following relief:

- Authorizing the installation and use, for a period of 30 days, of a pen register and trap and trace device on the **Subject Phones**; and

- Requiring service providers to furnish, for a 30-day period coinciding with the duration of the pen register authority requested in this Application, subscriber information for and subscriber information for telephone numbers in contact with the **Subject Phones**; and

- Requiring service providers to provide historical call detail records for the **Subject Phones** and records reflecting the cell tower and antenna face ("cell site") used at the start and end of each call for the **Subject Phones**, for the period from March 1, 2015, through July 24, 2015; and

- Requiring service providers to provide, for a period of 30 days, all information, facilities, and technical assistance needed to ascertain the physical location of the **Subject Phones** (the "Requested Location Information"),[1] and authorizing, for a period of 30 days, investigating agents to use a pen register, in the form of electronic investigative techniques that capture and analyze signals emitted by cellular telephones, including in private places, to ascertain the physical location of the **Subject Phones.**

UPON REVIEW OF THE APPLICATION, THIS COURT FINDS THAT:

The Applicant has certified that the information likely to be obtained by use of the pen register and trap and trace on the **Subject Phones**, with respect to telephone calls as well as direct connect, push-to-talk, and digital dispatch numbers, is relevant to an ongoing criminal investigation into offenses that include but are not necessarily limited to conspiracy to distribute narcotics, in violation of Title 21, United States Code, Sections 846 and 841(a), and money laundering, in violation of Title 18, United States Code, Sections 1957 and 1957 (the "Subject Offenses").

The government has represented that **Subject Phone 14** is used by UI5, that **Subject Phone 15** is used by UI6, and that the principal subjects of the aspect of the investigation presently before the Court are UI5 and UI6.

---

1 Such information shall include but not be limited to per call measurement data ("PCMD"), evolution data optimized ("EVDO"), Internet protocol detail record ("IPDR"), range-to-tower ("RTT"), tower distance information, data indicating the specific latitude and longitude and street address of the **Subject Phones**, as well as records reflecting the cell tower and antenna face used by the **Subject Phones** at the start and end of any call, and access through any means reasonably available to all location-based services with respect to the **Subject Phones**, such as "Enhanced 911," precision location information, mobile locator information, GPS, or "pinging."

Pursuant to Title 18, United States Code, Section 2703(d), the government has set forth specific and articulable facts showing that there are reasonable grounds to believe that subscriber information for and subscriber information for telephone numbers in contact with the **Subject Phones** is relevant and material to an ongoing criminal investigation.

Pursuant to Title 18, United States Code, Section 2703(d), the government has set forth specific and articulable facts showing that there are reasonable grounds to believe that historical call detail records for the **Subject Phones** and historical cell site information for the **Subject Phones** for the period from March 1, 2015, through July 24, 2015, are relevant and material to the ongoing drug trafficking investigation.

Pursuant to Title 18, United States Code, Section 2703(c)(1)(A) and Rule 41 of the Federal Rules of Criminal Procedure, the government has established probable cause to believe that information concerning the location of the **Subject Phones** at times determined by investigators will constitute or lead to evidence of the Subject Offenses.

Pursuant to Title 18, United States Code, Section 3103a(b), the Court finds that immediate notification of the execution of the Order requested by the government for the seizure of information concerning the location of the **Subject Phones** may have an adverse result, as defined in 18 U.S.C. § 2705(a)(2), namely flight from prosecution and otherwise seriously jeopardizing an investigation, that the facts of this case justify a period of delay in excess of 30 days, and that the

government has shown reasonable necessity for the seizure of such location information.

Upon consideration of the government's Application and the Court having found probable cause:

IT IS ORDERED, pursuant to Title 18, United States Code, Section 3123, that officers and employees of Homeland Security Investigations, and other authorized law enforcement officers, may install and use a pen register to record and decode dialing, routing, addressing, and signaling information transmitted by the **Subject Phones**, including direct connect, push-to-talk, and digital dispatch numbers, and also including "post-cut-through" digits, meaning those digits dialed from the **Subject Phones** after the initial call set-up is completed, subject to the limitations of 18 U.S.C. § 3121(c), to record the date and time of such transmissions, and to record the length of time the telephone receiver in question is off the hook for incoming or outgoing calls, for a period of 30 days, provided that Homeland Security Investigations shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing, routing, addressing, and signaling information utilized in the processing and transmission of wire or electronic communications so as not to include the contents of any wire or electronic communication.

IT IS FURTHER ORDERED, pursuant to Title 18, United States Code, Section 3123 that officers and employees of Homeland Security Investigations may direct Sprint/Nextel and any other communications service provider to install a trap

and trace device, including a caller identification feature known by the trade name "Caller ID Deluxe," on the **Subject Phones** to capture the incoming electronic or other impulses, including the originating telephone in call forwarding, terminating at the **Subject Phones**, which identify the originating number, or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of such incoming impulses, for a period of 30 days, and that the trap and trace device be without geographic limits, provided that Homeland Security Investigations shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing, routing, addressing, and signaling information utilized in the processing and transmission of wire or electronic communications so as not to include the contents of any wire or electronic communication.

IT IS FURTHER ORDERED, pursuant to Title 18, United States Code, Section 3123(b)(2), that Sprint/Nextel and any other communications service provider shall furnish officers and employees of Homeland Security Investigations forthwith all information, facilities, and technical assistance necessary to accomplish the installation and use of the pen register and trap and trace devices unobtrusively and with a minimum of interference with the services accorded to the party with respect to whom the installation and use is to take place.

IT IS FURTHER ORDERED, pursuant to Title 18, United States Code, Section 3127(3) and Rule 41 of the Federal Rules of Criminal Procedure, that officers and employees of Homeland Security Investigations, and other authorized

law enforcement officers, may employ electronic investigative techniques, for a period of 30 days, including in private places, to capture and analyze signals emitted by the **Subject Phones**, including in response to signals sent by law enforcement officers, at any time of the day or night, with the restriction that officers and employees of Homeland Security Investigations may neither retain nor make affirmative investigative use of the data acquired beyond that necessary to determine the location of the **Subject Phones**. Agents and employees of Homeland Security Investigations, and other authorized law enforcement officers, may send communications to the **Subject Phones** for the purpose of identifying the **Subject Phones** and its location.

IT IS FURTHER ORDERED that the government shall commence execution of this Order with respect to electronic investigative techniques that capture signals emitted by cellular telephones within 10 days.

IT IS FURTHER ORDERED that within 10 days after the termination of the execution of this Order with respect to electronic investigative techniques that capture signals emitted by cellular telephones, the government return this Order to the judge designated in this Order, together with an inventory advising this Court of the date and time that the techniques were first initiated and the period during which they were utilized.

IT IS FURTHER ORDERED, pursuant to Title 18, United States Code, Section 2703(d), that any service provider shall provide all information, facilities, and technical assistance necessary to determine the subscriber information set forth

in 18 U.S.C. § 2703(c)(2)(A)-(F), specifically, subscriber name, address, local and long distance telephone connection records, length of service (including start date) and types of services utilized, telephone or instrument number or other subscriber identification number (including but not limited to International Mobile Subscriber Identity number, Mobile Subscriber Identity Number, International Mobile Equipment Identity number, Universal Mobile Equipment Identity number, Electronic Serial Number, and Mobile Equipment Identity number), and means and source of payment for service (including any credit card or bank account number), for the **Subject Phones** and for telephone numbers in contact with the **Subject Phones**.

IT IS FURTHER ORDERED, pursuant to Title 18, United States Code, Section 2703(d), that Sprint/Nextel and any other communications service provider provide historical call detail records for the **Subject Phones** and further directing that Sprint/Nextel provide historical cell site information reflecting the cell tower and antenna face used at the start and end of each call, text message, and data transaction, including per call measurement data ("PCMD"), evolution data optimized ("EVDO"), Internet protocol detail record ("IPDR"), range-to-tower ("RTT") and tower distance information, for Subject Phone10 for the period from March 1, 2015 through July 24, 2015.

IT ISFURTHER ORDERED, pursuant to Title 18, United States Code, Section 2703(c)(1)(A) and Rule 41 of the Federal Rules of Criminal Procedure, that Sprint/Nextel and any other communications service provider, as defined in Section

2510(15) of Title 18, United States Code, shall assist agents of Homeland Security Investigations by providing all information, facilities and technical assistance to ascertain the physical location of the **Subject Phones** (the "Requested Location Information") for a period of 30 days.

IT IS FURTHER ORDERED that Sprint/Nextel and any other communications service provider, as defined in Section 2510(15) of Title 18, United States Code, shall disclose the Requested Location Information concerning the **Subject Phones**, and initiate a signal to determine the location of the **Subject Phones** on the service provider's network or with such other reference points as may be reasonably available and at such intervals and times as directed by Homeland Security Investigations, and shall furnish the technical assistance necessary to accomplish the acquisition unobtrusively and with a minimum of interference with such services as that provider affords the user of the **Subject Phones**, at any time of the day or night, good cause having been shown for obtaining such information outside of daytime hours.

IT IS FURTHER ORDERED that the government shall commence execution of this Order with respect to the seizure of the Requested Location Information within 10 days.

IT IS FURTHER ORDERED that within 10 days after the termination of the execution of this Order with respect to the seizure of the Requested Location Information, the government return this Order to the judge designated in this Order, together with an inventory advising this Court of the date and time that

acquisition of the Requested Location Information was first initiated and the period during which it was acquired.

IT IS FURTHER ORDERED, pursuant to Title 18, United States Code, Section 2706, that all service providers shall be compensated by the government at the prevailing rate for reasonable expenses incurred in furnishing the information, facilities and technical assistance necessary to comply with this Order, except, as provided in Title 18, United States Code, Section 2706(c), for providing records or other information maintained by the service provider that relate to telephone toll records and telephone listings.

IT IS FURTHER ORDERED that the furnishing of said information, facilities and technical assistance by service providers shall terminate after 30 days, measured from the earlier of the day on which service providers begin to furnish such assistance pursuant to this Order, or ten days from the date this Order is entered, unless otherwise ordered by this Court.

IT IS FURTHER ORDERED that no service provider, their representatives, agents, and employees, may disclose in any manner, directly or indirectly, by any action or inaction, to the listed subscriber for the **Subject Phones**, the subscribers of the incoming calls to or the outgoing calls from the **Subject Phones**, or to any person, the existence of the Court's order, in full or redacted form, or of this investigation unless ordered by this Court.

IT IS FURTHER ORDERED that this Court's orders and the application be sealed until further notice of this Court, except that copies of the Order to Service

Provider, in full or redacted form, may be served by law enforcement officers assisting in the investigation, on any service provider and their representatives, agents, and employees, as necessary to effectuate this Court's Order to Service Provider.

IT IS FURTHER ORDERED that pursuant to Rule 41(f)(3) and Title 18, United States Code, Section 3103a(b), the government may delay notification of the execution of any Order issued in this matter regarding the seizure of the location information with respect to the **Subject Phones** until October 21, 2015.

ENTERED:

RUBÉN CASTILLO
Chief Judge
United States District Court
Northern District of Illinois

DATED: 7/24/15