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