United States Court of Appeals

FOR THE DISTRICT OF COLUMBIA CIRCUIT

Argued December 3, 2015 Decided April 8, 2016

No. 12-3104

UNITED STATES OF AMERICA,
APPELLEE

v.

ERIC SCURRY, ALSO KNOWN AS E,
APPELLANT

Consolidated with 12-3105, 12-3109, 13-3055, 13-3068

Appeals from the United States District Court
for the District of Columbia
(No. 1:10-cr-00310-RCL-4)
(No. 1:10-cr-00310-RCL-7)
(No. 1:10-cr-00310-RCL-1)
(No. 1:10-cr-00310-RCL-2)
(No. 1:10-cr-00310-RCL-3)

Jonathan S. Zucker, appointed by the court, argued the cause for appellants Robert Savoy, et al. *Dennis M. Hart*, appointed by the court, argued the cause for appellant Eric Scurry. With them on the joint brief were *Pleasant S. Brodnax III*, *Howard B. Katzoff*, and *Mark Diamond*, all appointed by the court.

Daniel J. Lenerz, Attorney, U.S. Attorney's Office, argued the cause for appellee. On the brief were *Vincent H. Cohen Jr.*, Acting U.S. Attorney, and *Elizabeth Trosman*, *David B. Goodhand*, and *Arvind K. Lal*, Assistant U.S. Attorneys. *Elizabeth H. Danello*, Assistant U.S. Attorney, entered an appearance.

Before: ROGERS and PILLARD, *Circuit Judges*, and WILLIAMS, *Senior Circuit Judge*.

Opinion for the Court filed by *Circuit Judge* ROGERS.

ROGERS, *Circuit Judge*: The principal question presented in this appeal is whether Title III of the Omnibus Crime Control and Safe Streets Act of 1968 mandates suppression of evidence derived from a wiretap where information expressly required by the statute was omitted from the court order authorizing the wiretap. Appellants contend that the district court erred in denying their motions to suppress, relying on our subsequent decision in *United States v. Glover*, 736 F.3d 509 (D.C. Cir. 2013). In *Glover*, 736 F.3d at 513–14, the court reiterated the distinction drawn by the Supreme Court between two of the grounds for suppression of wiretap evidence under 18 U.S.C. § 2515. To determine whether an "unlawfully intercepted" communication merits suppression, *id.* § 2518(10)(a)(i), a court engages in "a broad inquiry into the government's intercept procedures to determine whether the government's actions transgressed the 'core concerns'" of Title III. *Glover*, 736 F.3d at 513. On the other hand, a mechanical test applies when a wiretap authorization order is "insufficient on its face," 18 U.S.C. § 2518(10)(a)(ii), and suppression is mandatory. *Glover*, 736 F.3d at 513–14. So, for example, in *Glover*, the court held suppression was mandatory under 18 U.S.C. §§ 2515 and 2518(10)(a)(ii) where the Title III authorization order was facially invalid because it exceeded the

limits of the district court's jurisdiction set forth in the statute, *id.* § 2518(3). *Glover*, 736 F.3d at 514–15. We hold that a wiretap order is "insufficient on its face," 18 U.S.C. § 2518(10)(a)(ii), where it fails to identify the Justice Department official who approved the underlying application, as required by Title III, *id.* § 2518(4)(d), accordingly reverse the denial of the motions to suppress evidence from wiretaps on the phones of appellants Terrance Hudson and Jerome Johnson, and remand. Otherwise we affirm, concluding appellants' other contentions lack merit.

I.

In July 2009, the Federal Bureau of Investigation ("FBI") began an investigation into narcotics trafficking in and around a group of multi-unit apartment buildings, "the Second Court," in the 4200 block of 4th Street in southeast Washington, D.C. Over the course of its investigation, the FBI identified a narcotics trafficking organization involved in distributing cocaine base (*i.e.*, crack cocaine) in the Second Court. The FBI, relying on information from two cooperating witnesses, concluded Eric Scurry was a Second Court crack dealer.

On April 2, 2010, the FBI submitted an application and proposed order, which was signed by the district court, for a 30-day wiretap on Scurry's cell phone, an order later extended for another 30-day period. Based on evidence obtained from Scurry's tapped calls, the FBI on June 11, 2010, applied for and received court authorization to tap two cell phones associated with Terrance Hudson, whom investigators had identified as part of the same narcotics-trafficking conspiracy as Scurry. Hudson's phone calls, in turn, suggested that Robert Savoy was one of his cocaine suppliers, and on July 22, 2010, the FBI obtained a wiretap court order for two cell phones associated with Savoy. Those wiretaps indicated that Savoy also supplied

crack and powder cocaine to another suspected narcotics dealer, James Brown. The Savoy wiretaps additionally indicated that Jerome Johnson supplied Savoy with large quantities of powder cocaine, and on September 10, 2010, the FBI sought and obtained a wiretap court order for Johnson's cell phone.

Appellants were indicted for various drug-trafficking offenses. After the district court denied their motions to suppress the wiretap evidence against them, *United States v. Savoy*, 883 F. Supp. 2d 101 (D.D.C. 2012), and Savoy's motion for reconsideration, appellants entered conditional guilty pleas pursuant to FED. R. CRIM. P. 11(a)(2). On appeal, they contend, relying on *Glover*, 736 F.3d 509, that Title III mandates suppression of evidence collected or derived from the wiretaps on Hudson and Johnson's cell phones because, as the district court found, *Savoy*, 883 F. Supp. 2d at 114, 120, the court orders authorizing those wiretaps were facially insufficient, *see* 18 U.S.C. § 2518(10)(a)(ii). They also contend that the district court erred in denying the motions to suppress evidence derived from the wiretaps on Scurry and Savoy's phones. "In evaluating appellants' objections to the district court's denial of . . . motions to suppress, we review the district court's legal conclusions de novo and its factual findings for clear error." *United States v. Eiland*, 738 F.3d 338, 347 (D.C. Cir. 2013).

II.

Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197, 211–25 (codified as amended at 18 U.S.C. §§ 2510 *et seq.*), sets forth a detailed procedure for the interception of wire, oral, or electronic communications, which is otherwise a felony, 18 U.S.C. § 2511; *cf. id.* §§ 2512–2513, and subject to civil penalties, *id.* § 2520. The procedure appears in 18 U.S.C. § 2518 (2012). Under Title III, a judge may authorize a wiretap by law enforcement officers

provided the application for and the court order authorizing the interception include certain specific information. *Id.* § 2518(1), (4).

The wiretap authorization process here entails four steps. *First*, the wiretap application must be pre-approved by one of the statutorily identified high-level Justice Department officials, specifically including the Attorney General, the Deputy Attorney General, the Associate Attorney General, any Assistant Attorney General, or any acting Assistant Attorney General, as well as certain Deputy Assistant Attorneys General specially designated by the Attorney General. *See id.* § 2516(1).

Second, the government must submit the application, under oath or affirmation, to a judge of competent jurisdiction and state the applicant's authority to make such application. *Id.* § 2518(1). Title III specifies what information the application must contain. *Id.* § 2518(1)(a)–(f). That information includes: (1) the identity of the high-level Justice Department official who approved the application ("the application identification requirement"), *id.* § 2518(1)(a); (2) an explanation of the facts and circumstances that the applying officer believes justify the wiretap, *id.* § 2518(1)(b); and (3) a statement describing the necessity of the wiretap to the government's investigation, *id.* § 2518(1)(c). "The judge may require the applicant to furnish additional testimony or documentary evidence in support of the application." *Id.* § 2518(2).

Third, before issuing the *ex parte* wiretap order, as requested or modified, a judge must make certain determinations based on the facts submitted by the applicant, *id.* § 2518(3), including that the wiretap is necessary to the investigation, *id.* § 2518(3)(c), and that there exists probable cause to believe that the phone to be tapped is or will soon be used in connection with particular enumerated criminal offenses, *id.* § 2518(3)(d).

Fourth, the judge issues an order approving the wiretap. Title III limits the length of the interception period to that "necessary to achieve" the wiretap's objective, with an initial maximum 30-day period subject to renewal upon submission of a new application. *Id.* § 2518(5). Title III also requires that the court order contain certain specified information. *Id.* § 2518(4)(a)–(e), (5). As relevant: The court order must specify "the nature and location of the communications facilities" to be wiretapped. *Id.* § 2518(4)(b). It must specify the identity of the high-level Justice Department official who approved the wiretap application ("the order identification requirement"). *Id.* § 2518(4)(d). And it must contain a provision mandating that law enforcement minimize the interception of communications that fall outside the scope of the wiretap order ("the minimization requirement"). *Id.* § 2518(5).

Title III includes its own exclusionary mandate. Section 2515 provides:

> Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of [Title III].

18 U.S.C. § 2515. A person seeking to enforce section 2515 must have Title III "standing," *see In re Evans*, 452 F.2d 1239, 1244 (D.C. Cir. 1971), which Title III defines as "[a]ny aggrieved person in any trial, hearing, or proceeding," 18 U.S.C. § 2518(10)(a), who was a target of the wiretap or a person party

to a wiretap intercept, *id.* § 2510(11). A person with standing may move to suppress wiretap evidence and its fruits on any of three grounds: "(i) the communication was unlawfully intercepted; (ii) the [wiretap] order . . . is insufficient on its face; or (iii) the interception was not made in conformity with the [wiretap] order . . . ." *Id.* § 2518(10)(a)(i)–(iii).

A.

No party disputes that the court orders authorizing the wiretaps on Hudson and Johnson's cell phones fail to identify the officials who pre-approved the underlying applications. The orders specify a type of official authorized to pre-approve wiretap applications, namely, a Deputy Assistant Attorney General in the Criminal Division specially designated by the Attorney General. *See id.* § 2516(1). But where that official's name should appear, there are only asterisks. The order authorizing the Hudson wiretap reads: the "application [was] authorized by ******, Deputy Assistant Attorney General of the Criminal Division, United States Department of Justice, pursuant to the power delegated to that official by special designation of the Attorney General." The order authorizing the Johnson wiretap states that the "application [was] authorized by *, Deputy Assistant Attorney General of the Criminal Division, United States Department of Justice, pursuant to the power delegated to that official by special designation of the Attorney General." There are five Deputy Assistant Attorneys General in the Criminal Division.[1] The district court ruled that the Hudson

[1] *See* U.S. Dep't of Justice, Justice Mgmt. Div., 2012 Organization, Mission and Functions Manual, *available at* https://www.justice.gov/archive/jmd/mps/2012/mission.htm (Criminal Division Organizational Chart dated Oct. 4, 2010); U.S. Dep't of Justice, Justice Mgmt. Div., Organization, Mission and Functions Manual, 2009, *available at* https://www.justice.gov/archive/jmd/mps/2009omf/mission.htm

and Johnson orders were facially insufficient for failing to comply with the identification requirement in section 2518(4)(d), but concluded, prior to *Glover*, that the facial insufficiency "constituted a technical defect that did not undermine the purposes of the [wiretap] statute or prejudice" Hudson or Johnson, and so denied their motions to suppress. *Savoy*, 883 F. Supp. 2d at 113–14, 120–21.

1. To determine whether a wiretap order is facially insufficient, a reviewing court must examine the four corners of the order and establish whether, on its face, it contains all that Title III requires it to contain. *See United States v. Chavez*, 416 U.S. 562, 573–74 (1974); *United States v. Giordano*, 416 U.S. 505, 525 n.14 (1974). If the order complies with the requirements of Title III, it is "[]sufficient on its face"; if it does not comply with those requirements, it is "insufficient on its face." *See* 18 U.S.C. § 2518(10)(a)(ii). For example, a wiretap order is facially sufficient when it names the Assistant Attorney General as the official who authorized the wiretap application even though extrinsic documents reveal that a different Justice Department official — *e.g.*, the Attorney General — authorized the application. *See Chavez*, 416 U.S. at 573–74. For purposes of section 2518(10)(a)(ii), then, it is enough that the official named in the order had the power to pre-approve wiretap applications.

There can be little question that each of the Hudson and Johnson orders is "insufficient on its face," *see* 18 U.S.C. § 2518(10)(a)(ii), because each fails to include information expressly required by Title III. Section 2518(4) enumerates certain categories of information that a wiretap order "shall specify." One is "the *identity* . . . of the person authorizing the application." *Id.* § 2518(4)(d) (emphasis added). The text is

---

(Criminal Division Organizational Chart dated Jan. 17, 2008).

plain and unambiguous; every wiretap court order must identify the individual high-level Justice Department official who, as required by section 2516(1), authorized the underlying wiretap application. This requirement may be met where the language points unambiguously to a unique qualified officer holding a position that only one individual can occupy at a time, but here there is more than one Deputy Assistant Attorney General and no individual Deputy is identified on the face of either the Hudson or the Johnson wiretap orders. This would appear to end this part of our inquiry. *See Engine Mfrs. Ass'n v. S. Coast Air Quality Mgmt. Dist.*, 541 U.S. 246, 252–54 (2004).

In resisting suppression, the government views the interpretation of sub-sections 2518(4)(d) and (10)(a)(ii) compelled by the text as adopting an overly formalistic approach. It urges the court to hold that a court wiretap order is not facially insufficient where essential information required by Title III is missing from the order so long as other materials submitted to the judge who issued the order supply the missing detail. Here, the application for the Hudson wiretap states that "Bruce C. Swartz, Deputy Assistant Attorney General of the Criminal Division, has authorized this Application" and includes as an attachment a copy of Deputy Swartz's signed letter approving the application. Similarly, the Johnson application includes as an attachment a signed letter of Kenneth A. Blanco, whom the letter identifies as a Deputy Assistant Attorney General in the Criminal Division, approving the application.

But, as noted, Title III's facial sufficiency inquiry is limited to the four corners of the wiretap order. *See Chavez*, 416 U.S. at 573–74; *Giordano*, 416 U.S. at 525 n.14. There is something incongruous about an interpretation that would let extrinsic documents transform an order that is "insufficient on its face" into one that is sufficient "on its face." *See* 18 U.S.C. § 2518(10)(a)(ii). Further, the government's interpretation

would allow it, in every case, to satisfy Title III's *order* identification requirement, *id.* § 2518(4)(d), by satisfying its *application* identification requirement, *id.* § 2518(1)(a), effectively rendering section 2518(4)(d) superfluous. *See Duncan v. Walker*, 533 U.S. 167, 174 (2001). Although Congress has amended Title III since its enactment in 1968, Congress has left unchanged the information required to be contained in a wiretap court order. *Compare* 18 U.S.C. § 2518(4)(a)–(e), *with* Title III, § 802, 82 Stat. at 219 (adding section 2518(4)(a)–(e) to Title 18).

To the extent Title III's two identification requirements are functionally redundant, it is clear that "Congress could sensibly have seen some practical value in the redundancy." *Gutierrez de Martinez v. Lamagno*, 515 U.S. 417, 445 (1995) (Souter, J., dissenting); *cf. Nat'l Ass'n of Clean Water Agencies v. EPA*, 734 F.3d 1115, 1126 (D.C. Cir. 2013). The deliberations leading up to the passage of Title III reveal deep unease over the risk to privacy interests inherent in granting wiretapping authority to law enforcement. With telecommunications technology — and alongside it eavesdropping technology — evolving rapidly, members of Congress feared that "if [Title III] is successful, today's narrowing enclave of individual privacy will shrink to the vanishing point." S. REP. NO. 90-1097, at 171 (1968) (additional views of Sen. Hart). The President and the Attorney General expressed serious misgivings about a wiretap statute, with the Attorney General testifying that wiretaps posed a risk to privacy "too great to permit their exploitation even by Government agents acting in the name of law enforcement." *Anti-Crime Program: Hearings Before Subcomm. No. 5 of the H. Comm. on the Judiciary*, 90th Cong. 209 (1967).

Congress sought, therefore, to limit the use of wiretaps — to balance law enforcement and privacy interests — by "impos[ing] important preconditions to obtaining any intercept

authority at all." *Giordano*, 416 U.S. at 515; *see also* Title III, § 801(a)–(d), 82 Stat. at 211–12. Among them was the requirement that a high-level Justice Department official sign off on each wiretap application. *See* 18 U.S.C. § 2516(1). Congress intended application pre-approval to "play a central role" in the Title III process, *Giordano*, 416 U.S. at 528, and to constitute "a critical precondition to any judicial order" authorizing a wiretap, *id.* at 516. According to the Report of the Senate Judiciary Committee, application pre-approval

> centralizes . . . the formulation of law enforcement policy on the use of electronic surveillance techniques. Centralization will avoid the possibility that divergent practices might develop. Should abuses occur, the lines of responsibility lead to an identifiable person. This provision in itself should go a long way toward guaranteeing that no abuses will happen.

S. REP. NO. 90-1097, at 97.

The identification requirements buttress this core bulwark against unwarranted intrusions into private conversations. As the Supreme Court has observed, "[t]here is little question that [the identification requirements] were intended to make clear who bore the responsibility for approval of the submission of a particular wiretap application." *Chavez*, 416 U.S. at 571–72; *see also* S. REP. NO. 90-1097, at 101, 103. This *ex post* check on the misuse or overuse of wiretaps, in turn, also operates as an *ex ante* constraint on executive branch conduct. Congress could reasonably conclude that a high-level Justice Department official, who is already prone to caution given the level of responsibilities attendant to the high position, will tread even more cautiously when reviewing proposed wiretap applications if the official is individually identified as having approved the application. Insisting on individual identification in both the

application and the order accords with Congress's intent "to make doubly sure that the statutory [wiretap] authority be used with restraint." *Giordano*, 416 U.S. at 515.

Furthermore, in functional terms, Title III's doubled identification requirements are not redundant. Title III contains evidence of Congress's intent that the order — independent of the application — be the operative document in the field. One sign of this intent is that all the information contained in the order is also contained in the application. *Compare* 18 U.S.C. § 2518(1)(a)–(b) & (d), *with id.* § 2518(4)(a)–(e). That complete overlap makes little sense if Congress expected the order always to travel with the application. Another indicator arises out of Title III's criminal and civil penalties. Since its enactment, Title III has exposed "any person" to personal-capacity civil liability, including punitive damages, and even criminal prosecution for carrying out an unlawful wiretap. 18 U.S.C. §§ 2511(1)(a)–(b), 2511(4)–(5), 2520(a)–(c); *see also* Title III, § 802, 82 Stat. at 213, 223. Good-faith reliance on a court order — but not on a wiretap application — is a complete defense to a criminal or civil action. 18 U.S.C. § 2520(d); *see also* Title III, § 802, 82 Stat. at 223. Congress expected reliance on the wiretap order in the field, where the risk of criminal and civil exposure is at its height, and it designed Title III's immunity provision accordingly. Practice confirms what Title III's design suggests. After the authorizing judge signs the wiretap order, the order — but not the application — goes to those involved in conducting the surveillance. The Hudson and Johnson orders, for example, state that the order, application, affidavit in support of the application, proposed orders, and interim reports be sealed, "except that copies of the orders, in full or redacted form, may be served on the [FBI] and its participating law enforcement agencies including the Metropolitan Police Department of the District of Columbia, and the service providers as necessary to effectuate this order."

Each identification requirement, then, has a distinct audience in the Title III process. "Requiring identification of the authorizing official in the application facilitates the court's ability to conclude that the application has been properly approved under § 2516 . . . ." *Chavez*, 416 U.S. at 575. Including that identification in the wiretap order facilitates additional oversight, this time by the parties executing the order. Congress did not want field agents or telecommunications service providers to conduct or assist in conducting wiretaps unless they — like the judge who authorized the wiretap — could satisfy themselves of proper compliance with section 2516(1)'s application pre-approval requirement. Section 2518(4)(d)'s order identification requirement is how Congress chose to furnish them evidence of compliance, thereby ensuring that the evidence would be at once fairly reliable, because a federal judge has vouched for its accuracy, and easily accessible, because it is included in the operative field document. And by tying immunity to good-faith reliance on a court order, *see* 18 U.S.C. § 2520(d), Congress created an incentive for field agents and service providers to examine a wiretap order for completeness, including the identity of the authorizing Justice Department official. With pre-approval as a critical check on the overuse or misuse of wiretapping authority, *see Giordano*, 416 U.S. at 516, 528, Congress designed Title III so that the absence of evidence of pre-approval by an individual Justice Department official at either of two stages would halt the wiretap process.

The government also contends that the Hudson and Johnson orders are facially sufficient because they identified the title of the person or the general category of official who authorized the underlying application. Alternatively, the government resorts to grammatical niceties. Each order states that the government sought the order "pursuant to an application authorized by . . . [a] Deputy Assistant Attorney General of the Criminal Division

. . . pursuant to the power delegated to *that official* by special designation of the Attorney General" (emphasis added). In the government's view, the use of the demonstrative adjective "that" before the noun "official" makes it reasonably believable that a single, individual Deputy Assistant Attorney General authorized the application.

The same reasoning undercuts both of the government's arguments. Title III requires that the wiretap order provide the "identity . . . of *the person*" who authorized the application. 18 U.S.C. § 2518(4)(d) (emphasis added). To specify a category of official or a job title is usually not the same thing as specifying the "identity" of a "person." Nor does it fix responsibility for approval of the wiretap application, *see* S. REP. NO. 90-1097, at 103, such that "[s]hould abuses occur, the lines of responsibility [would] lead to an *identifiable person*," *id.* at 97 (emphasis added). The same problems infect reliance on the reference to an unnamed Deputy Assistant Attorney General. As noted, five officials in the Criminal Division hold that title. Indeed, other documents show that two different Deputy Assistant Attorneys General — Swartz and Blanco — authorized the Hudson and Johnson wiretap applications. A third Deputy, John C. Keeney, authorized the application for a wiretap on Savoy's phone. That there is more than one Deputy Assistant Attorney General distinguishes the instant case from *United States v. Traitz*, 871 F.2d 368, 379 (3d Cir. 1989), where the failure to name *the* Assistant Attorney General for the Criminal Division, who had pre-approved the application, did not render the order facially insufficient; because at any given time, there is only one Assistant Attorney General for the Criminal Division, *see* 28 C.F.R. § 0.55 (referring to "*the* Assistant Attorney General, Criminal Division"), identifying that person by title is the functional equivalent of identifying the individual's name. Not so here.

Finally, the government contends that "[a]t worst, the authorizing orders' typographical errors rendered them 'imperfect' . . . but not facially insufficient." Appellee's Br. 26–27 (citing *Glover*, 736 F.3d at 515). The government is correct that *Glover*, 736 F.3d at 515, left open the possibility that a "technical defect" in a wiretap order might not rise to the level of facial insufficiency, but rather would render the order "imperfect." But the omissions in the Hudson and Johnson orders are not merely technical defects. The government failed to include in the proposed orders information expressly required by Title III. *See* 18 U.S.C. § 2518(4)(d). It is difficult to conceive of that as a technical defect. By contrast, the technical-defect cases the court cited in *Glover*, 736 F.3d at 515, did not involve facially insufficient orders that omitted information expressly required by Title III. *See United States v. Moore*, 41 F.3d 370, 372, 375–76 (8th Cir. 1994); *Traitz*, 871 F.2d at 378–79.

For these reasons, we agree with the district court that the Hudson and Johnson orders are facially insufficient under 18 U.S.C. § 2518(10)(a)(ii). *See Savoy*, 883 F. Supp. 2d at 113–14, 120–21.

.

2. The question remains whether suppression pursuant to section 2515 is the appropriate remedy here. "The issue does not turn on the judicially fashioned exclusionary rule aimed at deterring violations of Fourth Amendment rights, but upon the provisions of Title III." *Giordano*, 416 U.S. at 524. Title III sets out three grounds for suppression, 18 U.S.C. § 2518(10)(a)(i)–(iii), and the Supreme Court explained the analytical distinctions between them in *Chavez*, 416 U.S. at 573–75, and *Giordano*, 416 U.S. at 524–27. A functional inquiry determines whether a violation of Title III is such that the contents of the wiretap must be suppressed as "unlawfully intercepted." 18 U.S.C. § 2518(10)(a)(i). Suppression is

required only when the government fails to comply with "those statutory requirements that directly and substantially implement the congressional intention to limit the use of intercept procedures to those situations clearly calling for the employment of this extraordinary investigative device." *Giordano*, 416 U.S. at 527. Consequently, not every failure to comply with Title III will warrant suppression under section 2518(10)(a)(i). For example, under the "unlawfully intercepted" paragraph, the failure to comply with section 2516(1)'s application pre-approval requirement results in suppression, *Giordano*, 416 U.S. at 524–29, but suppression does not necessarily result from the misidentification of the authorizing Justice Department official in the wiretap application and order, *Chavez*, 416 U.S. at 574–80.

The Supreme Court, however, pursued an altogether different methodological tack in analyzing the scope of the facial-insufficiency ground of section 2518(10)(a)(ii). As this court recently explained, in *Giordano* and *Chavez*,

> the Court read paragraph (i) as requiring a broad inquiry into the government's intercept procedures to determine whether the government's actions transgressed the "core concerns" of the [wiretap] statute, whereas (ii) is a mechanical test; either the warrant is facially sufficient or it is not. . . . Suppression is the mandatory remedy when evidence is obtained pursuant to a facially insufficient warrant. There is no room for judicial discretion.

Glover, 736 F.3d at 513. In sum, once a reviewing court determines that a wiretap order is facially insufficient, the only appropriate remedy is suppression. Because the Hudson and Johnson wiretap orders are facially insufficient, *see supra* Part II.A.1, the contents of intercepts collected pursuant to those

orders and "evidence derived therefrom" must be suppressed. 18 U.S.C. §§ 2515, 2518(10)(a)(ii).

The government objects that the omissions in the Hudson and Johnson orders do not warrant suppression because the wiretap orders satisfy the functional "core concerns" test for suppression under the unlawfully intercepted ground of section 2518(10)(a)(i). That is, the record accompanying the wiretap applications submitted to the district court shows that a Deputy Assistant Attorney General in fact approved each of the applications. The Hudson and Johnson wiretaps therefore were not "unlawfully intercepted" within the meaning of section 2518(10)(a)(i). *See Chavez*, 416 U.S. at 574–80; *cf. Giordano*, 416 U.S. at 527–28. But that is irrelevant to the suppression inquiry under the facial-insufficiency ground of section 2518(10)(a)(ii). Title III provides for suppression in any one of three different circumstances, set forth in three separate subparagraphs separated by the disjunctive conjunction "or." 18 U.S.C. § 2518(10)(a). Suppression is required when the conditions set forth in *any* of those three paragraphs are met. That one paragraph does not require suppression has no bearing on the applicability of the other two. *Cf. Loughrin v. United States*, 134 S. Ct. 2384, 2389–90 (2014). What the government asks, in essence, is for the court to transform section 2518(10)(a) from a statutory provision establishing a disjunctive test into one establishing a conjunctive test. On the government's interpretation, a defendant would have to satisfy *all three* of its paragraphs to prevail on a motion to suppress. This is not the choice Congress made, and the government has pointed to nothing that supports a contrary conclusion.

The government's reliance on out-of-circuit cases declining to suppress wiretap evidence in circumstances like those here, *see* Appellee's Br. 20–22 n.11, is misplaced. In those cases, courts have reasoned that section 2518(10)(a)(i)'s "core

concerns" test can excuse orders that are facially insufficient under section 2518(10)(a)(ii). *See, e.g.*, *Traitz*, 871 F.2d at 379–80; *United States v. Robertson*, 504 F.2d 289, 291–92 (5th Cir. 1974); *United States v. Gray*, 521 F.3d 514, 524–28 (6th Cir. 2008); *United States v. Callum*, 410 F.3d 571, 574–76 (9th Cir. 2005); *United States v. Radcliff*, 331 F.3d 1153, 1161–63 (10th Cir. 2003). This panel is bound by the rejection of this approach in *Glover*, 736 F.3d at 513, where the court declined to import the "core concerns" test into the facial-insufficiency context. *See Belbacha v. Bush*, 520 F.3d 452, 457 (D.C. Cir. 2008); *LaShawn A. v. Barry*, 87 F.3d 1389, 1393 (D.C. Cir. 1996) (en banc). The *Glover* court's reasoning is, in any event, faithful to both Supreme Court precedent and the text of Title III.

For these reasons, we reverse the district court's denial of the motions to suppress the Hudson and Johnson wiretap evidence. *See Savoy*, 883 F. Supp. 2d at 113–14, 120–21. It remains for the district court on remand to determine the effect of our reversal on appellants' conditional pleas and what evidence is "derived" from the Hudson and Johnson wiretaps. *See* 18 U.S.C. § 2515. We note, parenthetically, that a number of cases cited by the government, Appellee's Br. 20–22 n.11, entail similar errors as here. The Justice Department can readily reduce the likelihood that it repeats this kind of error going forward. *Cf. Chavez*, 416 U.S. at 573 n.4. *The United States Attorneys' Manual*'s *Criminal Resource Manual* provides a detailed overview of what information a Title III order must contain. *See* DEP'T OF JUSTICE, U.S. ATTORNEYS' MANUAL: CRIMINAL RESOURCE MANUAL § 30 (2012), *available at* https://www.justice.gov/usam/criminal-resource-manual-30-electronic-surveillance-title-iii-orders. In fact, it includes every requirement enumerated in section 2518(4) except the requirement that the order identify the high-level Justice Department official who pre-approved the underlying

application. *Id.* A revision to the *Criminal Resource Manual* appears in order.

B.

Next, appellants contend that the district court erred by not interpreting the word "facilities" in sub-sections 2518(1)(b)(ii) and (4)(b) to require applications and orders for wiretaps on cell phones to identify the cell towers that will transmit signals to and from the tapped phone. We are not persuaded.

Title III requires that ordinary wiretap applications include "a particular description of the nature and *location* of the facilities from which or the place where the communication is to be intercepted." 18 U.S.C. § 2518(1)(b)(ii) (emphasis added). A wiretap order likewise must specify "the nature and *location* of the communications facilities as to which, or the place where, authority to intercept is granted." *Id.* § 2518(4)(b) (emphasis added). No party disputes that the wiretap applications and orders here identified the individual cell phones that would be subject to surveillance. Appellants maintain that the "location" of the "facilities" to be tapped must be geographically fixed and a cell phone, therefore, cannot constitute the "facilit[y]" to be tapped, because unlike a land-line telephone it has no fixed location. Instead, appellants contend that, in the cell phone context, the "location" of the "facilities" to be tapped is the cell tower — or, in reality, towers — through which the cell phone's signals are routed.

Title III does not define what is meant by the "facilities" targeted by the wiretap. But three considerations, based on the structure, purpose, and legislative history of Title III, *see N.Y. State Conference of Blue Cross & Blue Shield Plans v. Travelers Ins. Co.*, 514 U.S. 645, 655 (1995), persuade us that Congress intended the word "facilities" in sub-sections 2518(1)(b)(ii) and (4)(b) to encompass cell phones themselves. First, a contrary

interpretation would yield an absurd result. No Title III provision other than the "facilities" paragraphs — sub-sections 2518(1)(b)(ii) and (4)(b) — could be read to require that wiretap applications and orders identify the target phone. So if the target telephone is not a type of "facilit[y]," then wiretap applications and orders would never have to identify the specific phone the government intends to tap. Yet, Congress required applications and orders to specify the "nature and location" of the "facilities" to be tapped in order to "reflect[] the constitutional command of particularization" enshrined in the Fourth Amendment. S. REP. NO. 90-1097, at 101; *see also id.* at 102–03. The Fourth Amendment requires that a warrant "particularly describ[e] the place to be searched, and the persons or things to be seized." Generally, to satisfy the search component of the particularity requirement, a warrant must enable the executing officer to locate and identify the place to be searched and ensure — to a reasonable probability — that the officer will not mistakenly search the wrong place. *United States v. Johnson*, 437 F.3d 69, 73 (D.C. Cir. 2006). "In the wiretap context," the Fourth Amendment's particularity requirement is "satisfied by identification of the telephone line to be tapped and the particular conversations to be seized." *United States v. Donovan*, 429 U.S. 413, 427 n.15 (1977). Surely a Title III wiretap application or order could not satisfy the Fourth Amendment's particularity requirement if it failed to identify the individual phone to be tapped. Second, the Senate Judiciary Committee Report states that Congress understood telephones to be a type of "facilit[y]": "Subparagraph (b) [of section 2518(4)] requires the order to specify the *phone or other communication facilities* from which or the place where the authority to intercept is granted." S. REP. NO. 90-1097, at 102–03 (emphasis added); *see also id.* at 101. Third, of the many amendments to Title III since 1968, the parties point us to none — and we are aware of none — that suggests Congress intended Title III to treat wiretaps on cell phones differently

from wiretaps on land-line phones. Quite the contrary. In the Electronic Communications Privacy Act, Pub. L. No. 99-508, § 101(a)(1)(B), 100 Stat. 1848, 1848 (1986), Congress amended the definition of "wire communication" in Title III to "make[] clear that cellular communications — whether they are between two cellular telephones or between a cellular telephone and a 'land line' telephone — are included in the definition of 'wire communications' [sic] and are covered by [Title III]." S. REP. NO. 99-541, at 11 (1986); *see also* H.R. REP. NO. 99-647, at 31, 35 (1986).

Here, the information in the wiretap applications and orders at issue is sufficient to identify the "nature and location" of the targeted cell phones. Although Title III does not establish a minimum quantum of information necessary to identify the "nature and location" of a telephone targeted by a wiretap, the particularity requirement under the Fourth Amendment provides a useful guide to Congress' intent. *See* S. REP. NO. 90-1097, at 101–03. Each application and order specified the telephone number of the targeted cell phone, a serial number identifying the physical device associated with the target phone number, the identity of the service provider, and the name and address of the subscriber. With all of that information in hand, there is no basis to conclude an officer or service provider would find it difficult to identify the target phone or tap the wrong phone. *Cf. Johnson*, 437 F.3d at 73. Our sister circuits are in accord. *See United States v. Oliva*, 705 F.3d 390, 400–01 (9th Cir. 2012); *United States v. Goodwin*, 141 F.3d 394, 403 (2d Cir. 1997). Appellants' strained readings of Title III's definitions and case law interpreting other statutes are unavailing. It would be difficult to conclude from their arguments that Congress would resort to minor grammatical distinctions and subtle statutory alterations — with no accompanying explanation or comment — in order to institute as dramatic a change as a cell-phone carve out from Title III's ordinary requirements. Because the

applications and orders satisfied the facility-identification requirements of sub-sections 2518(1)(b)(ii) and (4)(b), the court need not address appellants' suggestion that the government ought to have complied with the more stringent requirements Title III imposes on so-called roving wiretaps. *See* 18 U.S.C. § 2518(11).

C.

Finally, appellants' challenges to the Scurry wiretaps are unpersuasive.

1. Appellants maintain that the application for the initial Scurry wiretap did not establish probable cause to believe the target phone was being or would be used to commit specified drug offenses. *See Savoy*, 883 F. Supp. 2d at 108–09. This challenge arises from the government's efforts to keep current on Scurry's cell phone habits. FBI Special Agent Christopher Fiorito had originally prepared an affidavit seeking a wiretap on a phone whose number ended in 9231 (the "9231 phone"). Fiorito abandoned that wiretap request, however, after he learned that Scurry had stopped using the 9231 phone. The wiretap application that was authorized was for a phone whose number ended in 7790 (the "target phone"). Appellants concede that the Fiorito affidavit furnishes probable cause to justify a wiretap on the 9231 phone, but object that the government failed to demonstrate probable cause to believe Scurry was using or would use the target phone to further his alleged narcotics-trafficking crimes. *See* 18 U.S.C. § 2518(1)(b), (3)(d).

Title III imports the Fourth Amendment's probable cause standard: the authorizing court must "make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before it, including the 'veracity' and 'basis of knowledge' of persons supplying hearsay information, there is a fair probability that contraband or evidence of a crime will

be found in a particular place." *Eiland*, 738 F.3d at 347 (alterations omitted) (quoting *Illinois v. Gates*, 462 U.S. 213, 238 (1983)). A reviewing court gives deference to the authorizing court's probable cause determinations. *Johnson*, 437 F.3d at 71.

The evidence proffered in the 56-page Fiorito affidavit demonstrates that there was a "fair probability" that the target phone was being and would be used to commit the specified narcotics offenses. Scurry and one of the government's cooperating witnesses ("Witness 2") had a months-long history of coordinating drug transactions by phone, including the 9231 phone. In February 2010, after federal agents had been investigating Scurry for several months, they learned from Witness 2 that Scurry had acquired a new phone, which they identified as the target phone. On March 11, Witness 2 received five calls from the target phone. During one of those calls, Scurry arranged to sell crack to Witness 2, a sale that took place the next day through one of Scurry's associates, acting at Scurry's behest. Around the same time Scurry began calling Witness 2 on the target phone, he largely stopped using the 9231 phone. Fiorito attests that, based on his experience, drug traffickers frequently switch phones to avoid police detection. Toll records revealed that the target phone was in contact with 75 phone numbers with which the 9231 phone had also been in contact. Of those, several numbers belonged to known associates of Scurry. According to Witness 2, another cooperating witness ("Witness 1"), and law enforcement surveillance, three of these associates were involved in selling drugs with or in the same area as Scurry. Although Witness 2 has had some veracity problems, Fiorito swore that Witness 1 was reliable and had never provided false information over three years of cooperating with the FBI.

Appellants hinge their challenge on a repeated error in the Fiorito affidavit. Specifically, the affidavit on several occasions incorrectly refers to the 9231 phone as the "target phone." Presumably, those mix-ups are artifacts of Fiorito's original affidavit, which was for a wiretap on the 9231 phone. In context, however, it is plain that the incorrect references to the "target phone" in fact describe the 9231 phone, and there is no reason to think these errors deceived the authorizing judge. The Fiorito affidavit states that Scurry was using the 9231 phone — and not the target phone — during the time period when it mistakenly refers to the 9231 phone as the "target phone," and several erroneous mentions of the "target phone" have as their clear referent an earlier mention of the 9231 phone. Nor is the Fiorito affidavit defective merely because it relied on some "boilerplate" language or a "cut and paste" from the earlier 9231 phone affidavit. *See* Appellants' Br. 54. "Even if the affidavit does contain some general language, applications are not to be read in a piecemeal fashion." *Eiland*, 738 F.3d at 347 (internal quotation marks omitted). Taken as a whole, then, the Fiorito affidavit satisfies Title III's probable cause requirement. *See* 18 U.S.C. § 2518(1)(b), (3)(d).

2. Appellants maintain that the district court erred when it determined that the Fiorito affidavit satisfied Title III's necessity requirement, *id.* § 2518(1)(c), (3)(c). *See Savoy*, 883 F. Supp. 2d at 109–10. Although intended to prevent over-reliance on wiretapping authority, Title III's necessity requirement "was not designed to foreclose electronic surveillance until every other imaginable method of investigation has been unsuccessfully attempted." *United States v. Carter*, 449 F.3d 1287, 1293 (D.C. Cir. 2006) (quoting *United States v. Williams*, 580 F.2d 578, 588 (D.C. Cir. 1978)). "[T]he government will meet its burden of demonstrating necessity if it shows that other techniques are impractical under the circumstances and that it would be unreasonable to require

pursuit of those avenues of investigation." *Id.* (internal quotation marks omitted). In the conspiracy context, the necessity requirement "is satisfied when 'traditional investigative techniques have proved inadequate to reveal the operation's full nature and scope.'" *United States v. (Ernest) Glover*, 681 F.3d 411, 420 (D.C. Cir. 2012) (quoting *United States v. Becton*, 601 F.3d 588, 596 (D.C. Cir. 2010)). This court reviews the authorizing judge's Title III necessity determination for abuse of discretion, although it does not grant additional deference to the district court's subsequent review. *See id.* at 419–20.

The Fiorito affidavit demonstrates that the authorizing judge did not abuse his discretion when he found that the first Scurry wiretap was necessary. Fiorito lists the investigative tools the FBI had already deployed, including physical surveillance, the use of confidential informants, analysis of pen-register and GPS-tracking data, and controlled narcotics purchases. But, he adds, these tools had failed to disclose the full nature and scope of the narcotics-trafficking enterprise operating in the Second Court. Physical surveillance, GPS tracking, and pen registers let the FBI know that Scurry was in contact with other potential suspects, but those tools told investigators little about the nature of Scurry's interactions. Confidential informants, for their part, had limited access to co-conspirators. Fiorito also attests to the insufficiency of investigative techniques short of a wiretap. A number of techniques risked revealing the existence of the investigation to its targets and putting government cooperators in harm's way: interviews with Scurry's associates, a search of one of Scurry's stash houses, trash pulls, and arranging for a cooperator to introduce Scurry to an undercover officer. Scurry's anti-surveillance countermeasures had frustrated attempts to use still other investigative techniques. Scurry took evasive maneuvers to avoid physical surveillance, consummated drug sales indoors or inside cars, and insulated himself from

people he did not know, like undercover officers. To secure useful grand jury testimony, the government would likely have had to immunize the investigation's targets, which would defeat the purpose of securing their testimony. This court has repeatedly upheld necessity determinations based on affidavits similar to the Fiorito affidavit. *See, e.g.*, *Eiland*, 738 F.3d at 348–49; *(Ernest) Glover*, 681 F.3d at 420; *Carter*, 449 F.3d at 1293–94; *Becton*, 601 F.3d at 596–97.

Appellants' counterarguments amount to little more than second-guessing how the government ought to run its investigations and prosecute drug crimes. They maintain that the government could have searched Scurry's known stash house or prosecuted Scurry on the evidence of controlled narcotics transactions alone. That assertion runs counter to the law of this circuit on the scope of Title III's necessity requirement in the conspiracy context. *See (Ernest) Glover*, 681 F.3d at 420. Appellants also challenge the Fiorito affidavit on the ground that it failed to mention an earlier, unsuccessful prosecution of Scurry on drug charges. The fact of the earlier prosecution, they contend, might have led the authorizing judge to take a different view of whether the wiretap was necessary. Moreover, appellants suggest, it might have led the judge to worry that a desire for retribution — rather than necessity — lay behind the government's wiretap application. Appellants never raised this argument in the district court. *See* Scurry Mot. to Suppress at 5–6 (Oct. 14, 2011); *Savoy*, 883 F. Supp. 2d at 109–10. Although our precedent is unclear as to the appropriate standard of review in these circumstances, *compare Eiland*, 738 F.3d at 350, *with United States v. Peyton*, 745 F.3d 546, 551 (D.C. Cir. 2014), under any standard appellants' challenge fails. If anything, the government's loss in the first case — a comparably simple case involving two counts of distribution — underscores the need for additional investigative tools. As for

evidence suggesting retributive motivation or bias on the government's part, appellants point to none.

3. Appellants maintain that the agents executing the Scurry wiretaps failed to comply with Title III's minimization requirement, 18 U.S.C. § 2518(5). Such compliance turns on whether the government made "reasonable efforts to minimize interceptions of non-pertinent communications." *Carter*, 449 F.3d at 1295. In appellants' view, the FBI listened to too many non-pertinent calls for too long to have taken reasonable steps to minimize such interceptions. As the district court held, *Savoy*, 883 F. Supp. 2d at 110–11, this argument is foreclosed by controlling precedent. *See Scott v. United States*, 436 U.S. 128, 139–41 (1978); *Carter*, 449 F.3d at 1295. More to the point, in *United States v. Cano-Flores*, 796 F.3d 83, 87–88 (D.C. Cir. 2015), the court rejected the argument appellants advance. To challenge the reasonableness of the government's minimization efforts, a party must present more than the raw number of non-pertinent intercepted calls and their durations.

Accordingly, we reverse the denial of the motions to suppress the Hudson and Johnson wiretap evidence, remand the case for further proceedings, and otherwise affirm.