

No. 17-43

In the Supreme Court of the United States

LOS ROVELL DAHDA, PETITIONER

v.

UNITED STATES OF AMERICA

*ON WRIT OF CERTIORARI
TO THE UNITED STATES COURT OF APPEALS
FOR THE TENTH CIRCUIT*

BRIEF FOR THE UNITED STATES

NOEL J. FRANCISCO
*Solicitor General
Counsel of Record*

JOHN P. CRONAN
*Acting Assistant Attorney
General*

MICHAEL R. DREEBEN
Deputy Solicitor General

ERIC J. FEIGIN
ZACHARY D. TRIPP
*Assistants to the Solicitor
General*

FINNUALA K. TESSIER
*Attorney
Department of Justice
Washington, D.C. 20530-0001
SupremeCtBriefs@usdoj.gov
(202) 514-2217*

QUESTION PRESENTED

Whether evidence obtained in conformity with the substantive requirements of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 211, must be suppressed because the orders authorizing its interception erroneously purported also to authorize interception beyond the issuing court's territorial jurisdiction.

TABLE OF CONTENTS

| | Page |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|
| Opinions below | 1 |
| Jurisdiction | 1 |
| Statutory provisions involved | 1 |
| Statement | 2 |
| Summary of argument | 12 |
| Argument..... | 15 |
| A. The Title III orders in this case were overbroad, not “insufficient” | 16 |
| B. Suppression is unwarranted because the mistake in the orders is not a fundamental defect..... | 19 |
| 1. Title III requires suppression for facial errors only when they are sufficiently fundamental to prevent the government from relying on the order to conduct interception..... | 19 |
| 2. The legal mistake in the orders here did not prevent the government from relying on them to intercept communications over the tapped phones..... | 24 |
| C. Any insufficiency arising from the overbreadth of the orders in this case would be severable..... | 31 |
| Conclusion | 41 |
| Appendix — Statutory provisions..... | 1a |

TABLE OF AUTHORITIES

Cases:

| | |
|---------------------------------------------------------------|--------|
| <i>Aday v. Superior Court</i> , 362 P.2d 47 (Cal. 1961) | 34 |
| <i>Arizona v. Evans</i> , 514 U.S. 1 (1995)..... | 29 |
| <i>Davis v. United States</i> , 564 U.S. 229 (2011) | 29 |
| <i>Groh v. Ramirez</i> , 540 U.S. 551 (2004) | 18 |
| <i>Herring v. United States</i> , 555 U.S. 135 (2009) | 29, 36 |
| <i>Hudson v. Michigan</i> , 547 U.S. 586 (2006) | 35, 36 |
| <i>Illinois v. Krull</i> , 480 U.S. 340 (1987) | 36 |

IV

| Cases—Continued: | Page |
|--------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| <i>Murray v. United States</i> , 487 U.S. 533 (1988)..... | 33 |
| <i>Nix v. Williams</i> , 467 U.S. 431 (1984) | 33 |
| <i>Pennsylvania Bd. of Prob. & Parole v. Scott</i> , 524 U.S. 357 (1998)..... | 35 |
| <i>People v. Defore</i> , 150 N.E. 585 (N.Y.), cert. denied, 270 U.S. 657 (1926)..... | 40 |
| <i>Sanchez-Llamas v. Oregon</i> , 548 U.S. 331 (2006)..... | 29 |
| <i>Schindler Elevator Corp. v. United States ex rel.</i> <i>Kirk</i> , 563 U.S. 401 (2011) | 16 |
| <i>Steel Co. v. Citizens for a Better Env't</i> , 523 U.S. 83 (1998)..... | 30 |
| <i>United States v. Barajas</i> , 710 F.3d 1102 (10th Cir.), cert. denied, 134 S. Ct. 230 (2013) | 30 |
| <i>United States v. Calandra</i> , 414 U.S. 338 (1974)..... | 36 |
| <i>United States v. Chavez</i> , 416 U.S. 562 (1974) | 19, 20 |
| <i>United States v. Christine</i> , 687 F.2d 749 (3d Cir. 1982) | 34 |
| <i>United States v. Cunningham</i> , 113 F.3d 289 (1st Cir.), cert. denied, 522 U.S. 862 (1997)..... | 38 |
| <i>United States v. Donovan</i> , 429 U.S. 413 (1977) ... | 5, 20, 21, 26 |
| <i>United States v. Giordano</i> , 416 U.S. 505 (1974)..... | <i>passim</i> |
| <i>United States v. Glover</i> , 736 F.3d 509 (D.C. Cir. 2013) | 39 |
| <i>United States v. Grubbs</i> , 547 U.S. 90 (2006)..... | 16 |
| <i>United States v. Holden</i> , 603 Fed. Appx. 744 (11th Cir.), cert. denied, 136 S. Ct. 522 (2015), and 136 S. Ct. 851 (2016)..... | 38 |
| <i>United States v. Houston</i> , 665 F.3d 991 (8th Cir.), cert. denied, 566 U.S. 1004 (2012) | 29 |
| <i>United States v. Jones</i> , 565 U.S. 400 (2012)..... | 27 |
| <i>United States v. Krueger</i> , 809 F.3d 1109 (10th Cir. 2015)..... | 29 |

V

| Cases—Continued: | Page |
|--------------------------------------------------------------------------------------------------------------------------|----------------|
| <i>United States v. Leon</i> , 468 U.S. 897 (1984)..... | 18, 28, 29, 36 |
| <i>United States v. Lomeli</i> , 676 F.3d 734 (8th Cir. 2012)..... | 24 |
| <i>United States v. Malekzadeh</i> , 855 F.2d 1492 (11th Cir. 1988), cert. denied, 489 U.S. 1029 (1989)..... | 30 |
| <i>United States v. Moore</i> , 41 F.3d 370 (8th Cir. 1994)..... | 38 |
| <i>United States v. Ojeda Rios</i> , 495 U.S. 257 (1990) | 28 |
| <i>United States v. Pitts</i> , 173 F.3d 677 (8th Cir. 1999)..... | 34 |
| <i>United States v. Radcliff</i> , 331 F.3d 1153 (10th Cir.), cert. denied, 540 U.S. 973 (2003) | 10, 38 |
| <i>United States v. Ramirez</i> , 112 F.3d 849 (7th Cir.), cert. denied, 522 U.S. 892 (1997) | 7, 14, 25 |
| <i>United States v. Rodriguez</i> , 968 F.2d 130 (2d Cir.), cert. denied, 506 U.S. 847, and 506 U.S. 1023 (1992)..... | 6 |
| <i>United States v. Scurry</i> , 821 F.3d 1 (D.C. Cir. 2016)..... | 5, 39 |
| <i>United States v. Sells</i> , 463 F.3d 1148 (10th Cir. 2006), cert. denied, 549 U.S. 1229 (2007) | 33, 39 |
| <i>United States v. Soto-Camargo</i> , No. 14-cr-40129, 2015 WL 3823020 (D. Kan. June 19, 2015)..... | 7 |
| <i>United States v. Vasquez-Garcia</i> , No. 10-40014, 2014 WL 7359490 (D. Kan. Dec. 23, 2014)..... | 7 |
| <i>Utah v. Strieff</i> , 136 S. Ct. 2056 (2016)..... | 33 |
| <i>Waller v. Georgia</i> , 467 U.S. 39 (1984)..... | 34 |
| <i>Wong Sun v. United States</i> , 371 U.S. 471 (1963) | 33 |

Constitution, statutes, and rule:

U.S. Const.:

| | |
|---------------------------------------------------------------------------------------------------------|--------------------|
| Art. III, § 1..... | 27 |
| Amend. IV..... | 27, 28, 34, 36, 39 |
| Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, Tit. III, 82 Stat. 211 | 4 |
| 18 U.S.C. 2510(4) | 6, 1a |
| 18 U.S.C. 2510(12) | 40, 3a |

VI

| Statutes and rule—Continued: | Page |
|---------------------------------------------------|----------------------------|
| 18 U.S.C. 2515..... | 8, 32, 7a |
| 18 U.S.C. 2516..... | 4, 15a |
| 18 U.S.C. 2518(1)..... | 4, 15a |
| 18 U.S.C. 2518(1)(a)..... | 23, 15a |
| 18 U.S.C. 2518(1)(b)(iv)..... | 21, 15a |
| 18 U.S.C. 2518(3)..... | <i>passim</i> , 16a |
| 18 U.S.C. 2518(4)..... | 5, 6, 13, 17, 22, 23, 17a |
| 18 U.S.C. 2518(4)(b)..... | 5, 36, 17a |
| 18 U.S.C. 2518(4)(d)..... | 23, 17a |
| 18 U.S.C. 2518(4)(e)..... | 24, 35, 36, 18a |
| 18 U.S.C. 2518(5)..... | 5, 37, 18a |
| 18 U.S.C. 2518(8)(a)..... | 28, 21a |
| 18 U.S.C. 2518(8)(d)..... | 21, 22a |
| 18 U.S.C. 2518(10)(a)..... | 9, 19, 23, 40, 23a |
| 18 U.S.C. 2518(10)(a)(i)..... | 9, 13, 20, 21, 32, 38, 23a |
| 18 U.S.C. 2518(10)(a)(ii)..... | <i>passim</i> , 23a |
| 18 U.S.C. 2518(10)(a)(iii)..... | 32, 23a |
| 18 U.S.C. 2..... | 2 |
| 21 U.S.C. 841(a)(1)..... | 2, 3 |
| 21 U.S.C. 841(b)(1)(A) (2006 & Supp. V 2011)..... | 2 |
| 21 U.S.C. 841(b)(1)(D)..... | 2, 3 |
| 21 U.S.C. 843(b)..... | 2 |
| 21 U.S.C. 846..... | 2, 3 |
| 21 U.S.C. 856..... | 2 |
| 21 U.S.C. 856(a)(1)..... | 2 |
| 21 U.S.C. 856(a)(2)..... | 2 |
| 21 U.S.C. 860..... | 3 |
| 47 U.S.C. 1002(a)(1)..... | 6 |
| Fed. R. Crim. P. 52(a)..... | 40 |

VII

| Miscellaneous: | Page |
|-------------------------------------------------------------------------------------------------------|-------------------|
| 2 Wayne R. LaFave, <i>Search and Seizure: A Treatise on the Fourth Amendment</i> (5th ed. 2012) | 33, 34, 35 |
| 5 <i>Oxford English Dictionary</i> (1933)..... | 16 |
| S. Rep. No. 1097, 90th Cong., 2d Sess. (1968)..... | 5, 17, 32, 33, 36 |
| <i>Webster's New International Dictionary</i> (2d ed. 1958)..... | 16 |
| <i>Webster's Third New International Dictionary</i> (2002)..... | 16, 32 |

In the Supreme Court of the United States

No. 17-43

LOS ROVELL DAHDA, PETITIONER

v.

UNITED STATES OF AMERICA

*ON WRIT OF CERTIORARI
TO THE UNITED STATES COURT OF APPEALS
FOR THE TENTH CIRCUIT*

BRIEF FOR THE UNITED STATES

OPINIONS BELOW

The opinion of the court of appeals (Pet. App. 1a-31a) in petitioner Los Dahda's case is reported at 853 F.3d 1101. The opinion of the court of appeals in petitioner Roosevelt Dahda's case (Pet. App. 32a-58a) is reported at 852 F.3d 1282. The order of the district court (Pet. App. 59a-65a) is unreported.

JURISDICTION

The judgments of the court of appeals in both cases were entered on April 4, 2017. The petition for a writ of certiorari was filed on July 3, 2017, and the petition was granted on October 16, 2017. The jurisdiction of this Court rests on 28 U.S.C. 1254(1).

STATUTORY PROVISIONS INVOLVED

Pertinent statutory provisions are reproduced in an appendix to this brief. See App., *infra*, 1a-26a.

STATEMENT

Following a jury trial in the United States District Court for the District of Kansas, petitioner Los Dahda was convicted of conspiracy to possess with intent to distribute and distribute five kilograms or more of cocaine, to manufacture, possess with intent to distribute, and distribute 1000 kilograms or more of marijuana, and to maintain drug-involved premises, in violation of 21 U.S.C. 841(a)(1), 846, 856, and 21 U.S.C. 841(b)(1)(A) (2006 & Supp. V 2011); two counts of distribution of marijuana, in violation of 21 U.S.C. 841(a)(1), (b)(1)(D), and 18 U.S.C. 2; maintenance of drug-involved premises, in violation of 21 U.S.C. 856(a)(1), (a)(2), and 18 U.S.C. 2; six counts of use of a communication facility to facilitate a drug-trafficking offense, in violation of 21 U.S.C. 843(b); three counts of possession with intent to distribute marijuana, in violation of 21 U.S.C. 841(a)(1), (b)(1)(D), and 18 U.S.C. 2; and attempted possession with intent to distribute marijuana, in violation of 21 U.S.C. 841(a)(1), (b)(1)(D), 846, and 18 U.S.C. 2. J.A. 68-71. He was sentenced to 189 months of imprisonment, to be followed by ten years of supervised release. J.A. 71-72. The court of appeals affirmed. Pet. App. 1a-31a.

Following the same trial, petitioner Roosevelt Dahda was convicted of conspiracy to possess with intent to distribute and distribute five kilograms or more of cocaine, to manufacture, possess with intent to distribute, and distribute 1000 kilograms or more of marijuana, and to maintain drug-involved premises, in violation of 21 U.S.C. 841(a)(1), 846, and 21 U.S.C. 841(b)(1)(A) (2006 & Supp. V 2011); five counts of use of a communication facility to facilitate a drug-trafficking offense, in violation of 21 U.S.C. 843(b); two counts of possession with intent to distribute marijuana, in violation of

21 U.S.C. 841(a)(1) and (b)(1)(D); possession with intent to distribute and distribution of marijuana within 1000 feet of a protected zone (playground), in violation of 21 U.S.C. 841(a)(1), (b)(1)(D), and 860; and attempted possession with intent to distribute marijuana, in violation of 21 U.S.C. 841(a)(1), (b)(1)(D), and 846. J.A. 80-83. He was sentenced to 201 months of imprisonment, to be followed by ten years of supervised release. J.A. 83-85. The court of appeals affirmed. Pet. App. 32a-58a.

1. In 2006, Chad Bauman, Peter Park, and Wayne Swift began working together to distribute marijuana in Kansas. Pet. App. 3a. Petitioner Los Dahda joined the network as an importer and a dealer. *Ibid.* Among other things, he drove money from Kansas to California to buy the marijuana, helped with the purchase and packaging of marijuana in California, loaded marijuana into crates for shipment to Kansas, and sold the marijuana in Kansas to redistributors. *Id.* at 3a-4a. His twin brother, petitioner Roosevelt Dahda, assisted him in a variety of ways, including by selling “pounds of marijuana” in Kansas, picking up shipments of marijuana from the warehouse in Kansas, and transporting cash to California to pay for drugs. *Id.* at 35a-36a.

“The network operated for roughly seven years, but the relationships and work assignments varied over time.” Pet. App. 4a. For example, when a dispute arose, Bauman stopped working with Park and Swift. *Ibid.* Nonetheless, petitioner Los Dahda continued to work with Bauman “to acquire marijuana in California and to transport [it] to Kansas for distribution there.” *Ibid.* Approximately one year later, Los Dahda stopped working with Bauman and resumed working with Park and Swift to acquire marijuana from California and in Kansas. *Ibid.*

2. As part of its investigation into the drug network, the government submitted applications to the United States District Court for the District of Kansas for orders authorizing the interception of wire and electronic communications over cellphones used by petitioners and other suspected members of the network. See Pet. App. 14a. The government sought those orders pursuant to Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 211, which “prescribes the procedure for securing judicial authority to intercept wire [oral or electronic] communications in the investigation of specified serious offenses.” *United States v. Giordano*, 416 U.S. 505, 507 (1974). The district court issued ten orders authorizing interceptions over 11 target cellphones, five of which belonged to petitioners. See J.A. 93-178 (reproducing orders); see also J.A. 95, 103-104, 122, 131, 157 (target phones used by petitioners).

a. Title III authorizes a judge, upon a proper application from the government, 18 U.S.C. 2518(1), to issue a wiretap order “if the judge determines,” among other things, that the application shows that probable cause exists that a sufficiently serious offense listed in 18 U.S.C. 2516 has been or will be committed; that probable cause exists that interception will obtain communications about that offense; and that “normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous.” 18 U.S.C. 2518(3). Petitioners do not dispute that the government’s applications in this case were proper, that the issuing court made the requisite judicial determinations, or that its determinations were correct.

Title III provides that an order authorizing interception over a cellphone “shall specify” (a) the target’s identity, if known; (b) the target cellphone number or other unique identifier;¹ (c) the type of communications to be intercepted and the crime to which the communications relate; (d) the agency authorized to intercept the communications and the official who approved the government’s application for the wiretap order; and (e) the period of time during which interception is permitted, not to exceed 30 days absent an extension. 18 U.S.C. 2518(4); see 18 U.S.C. 2518(5). Petitioners do not dispute that the orders in this case contained all of the required specifications.

b. Title III does not require that an order specify the locations where interception over a cellphone may occur. Rather than mandating that each order contain a case-specific judicial determination on that subject, the statute instead addresses the issue in its text.

Title III describes the order that a court “may enter” as “authorizing or approving interception * * * within the territorial jurisdiction of the court in which the judge is sitting (and outside that jurisdiction but within

¹ The statute provides that an order must specify “the nature and location of the communications facilities.” 18 U.S.C. 2518(4)(b). It is well-settled, and petitioners do not dispute, that the “communication[] facilit[y]” is the tapped cellphone and that its “nature and location” are given by its phone number or other unique identifier, like an international mobile subscriber identity (IMSI) number. See *United States v. Scurry*, 821 F.3d 1, 14-15 (D.C. Cir. 2016); S. Rep. No. 1097, 90th Cong., 2d Sess. 102-103 (1968) (Section 2518(4)(b) “requires the order to specify the phone or other communication facilities from which or the place where the authority to intercept is granted.”); see also *United States v. Donovan*, 429 U.S. 413, 437 (1977) (this requirement was “intended to reflect what Congress perceived to be the constitutional command of particularization”).

the United States in the case of a mobile interception device authorized by a Federal court within such jurisdiction.” 18 U.S.C. 2518(3). Title III defines “intercept” to include “the aural or other acquisition of the contents of any * * * communication.” 18 U.S.C. 2510(4). It is undisputed that interception occurs in the place “where the tapped phones are located” or the place “where officers put their listening post.” Pet. Br. 11 (quoting Pet. App. 16a-17a); *e.g.*, *United States v. Rodriguez*, 968 F.2d 130, 136 (2d Cir.) (where “the to-be-tapped telephone is located” or “where the contents of a wire communication are first to be heard and understood by human ears, other than those of the parties to the conversation”), cert. denied, 506 U.S. 847, and 506 U.S. 1023 (1992).

The parties here agree that interception “outside” the territorial jurisdiction of the court that issued the order, “in the case of a mobile interception device,” 18 U.S.C. 2518(3), applies only when the government employs an interception device that is itself mobile, like a bug installed in a car. See Pet. App. 18a-20a.² Some courts have held, however, that a tapped mobile phone itself always qualifies as a “mobile interception device,”

² In practice, the government no longer uses mobile interception devices to intercept cellphone communications in Title III cases. When the government obtains a court order authorizing interception, it becomes entitled to orders mandating “technical assistance necessary to accomplish the interception.” 18 U.S.C. 2518(4). And Congress has required telecommunications carriers to maintain the capability to enable law enforcement, pursuant to a court order, to intercept wire and electronic communications. 47 U.S.C. 1002(a)(1). The government now uses technical-assistance orders to have the cellular service provider transmit communications over a target phone to law enforcement, where they are first heard or read—and thus intercepted—in a wire room.

so the government may lawfully intercept communications at a wire room located outside the court's jurisdiction even when the mobile phone is also outside the court's jurisdiction. *E.g.*, *United States v. Ramirez*, 112 F.3d 849, 853 (7th Cir.), cert. denied, 522 U.S. 892 (1997); *United States v. Soto-Camargo*, No. 14-cr-40129, 2015 WL 3823020, at *2-*4 (D. Kan. June 19, 2015) (following *Ramirez*); *United States v. Vasquez-Garcia*, No. 10-40014, 2014 WL 7359490, at *2-*4 (D. Kan. Dec. 23, 2014) (same).

The district court that issued the orders in this case apparently adopted the latter view, which it memorialized in the orders here. Each order states:

Pursuant to Title 18, United States Code § 2518(3), it is further Ordered that, in the event [the target cellphones] are transported outside the territorial jurisdiction of the court, interception may take place in any other jurisdiction within the United States.

E.g., J.A. 97.³

The orders thus authorized many interceptions that would comply with Title III, as well as some that would not. Consistent with Title III, the orders allowed interception to occur whenever a tapped cellphone was inside Kansas, the government was listening from inside Kansas, or a tapped cellphone was outside Kansas and the government was listening from outside Kansas by using a mobile interception device. The orders also, however, purported to allow interception beyond Title III's limitations, in the event a tapped cellphone was outside Kansas and the government was listening at a wire

³ This same language appeared in the government's applications for the orders. *E.g.*, *Los Dahda C.A.* ROA Supp. Vol. IV, at 57.

room outside Kansas without using a mobile interception device.

c. For ten of the 11 tapped phones, the government listened from a wire room in Overland Park, Kansas. J.A. 46-47. It is undisputed that all of those interceptions were substantively lawful. For the remaining phone (target phone #7, belonging to Phillip Alarcon), the government listened from a wire room at the headquarters of the Drug Enforcement Administration in St. Louis, Missouri, while Alarcon was in California. J.A. 47-49. The government did not intercept any of the communications by using a mobile interception device.

3. Petitioners were indicted on multiple drug-trafficking counts, and the government subsequently sought to introduce at trial some of the interceptions “from [its] listening post in Kansas, i.e., within the jurisdiction of this issuing court.” Pet. App. 68a. It did not seek to introduce any interceptions over Alarcon’s phone. See *id.* at n.7 (noting that petitioners’ “motion is moot as to Target Telephone 7”); J.A. 54 (district court stating that “target telephone seven is essentially moot, since the government concedes it’s not going to use any of the evidence”). Petitioners filed a motion to suppress the interceptions made at the Kansas listening post, which the district court denied. Pet. App. 14a.

a. Title III provides that, “[w]henver 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 * * * if the disclosure of that information would be in violation of this chapter.” 18 U.S.C. 2515. “What disclosures are forbidden, and are subject to motions to suppress, is in turn governed by [18 U.S.C.] 2518(10)(a).” *Giordano*, 416 U.S. at 524.

Section 2518(10)(a) states that a defendant “may move to suppress the contents of any wire or oral communication intercepted pursuant to this chapter, or evidence derived therefrom,” on the grounds that:

- (i) the communication was unlawfully intercepted;
- (ii) the order of authorization or approval under which it was intercepted is insufficient on its face; or
- (iii) the interception was not made in conformity with the order of authorization or approval.

18 U.S.C. 2518(10)(a). “If the motion is granted, the contents of the intercepted wire or oral communication, or evidence derived therefrom, shall be treated as having been obtained in violation of this chapter.” *Ibid.*

b. Petitioners’ suppression motion did not contend that any of the wiretap evidence used at trial, all of which was intercepted in the Kansas wire room, was “unlawfully intercepted,” 18 U.S.C. 2518(10)(a)(i). Petitioners instead contended that the orders were “insufficient on [their] face,” 18 U.S.C. 2518(10)(a)(ii), because they were overbroad in respect to the circumstances in which they purported to authorize interception outside Kansas, see Pet. App. 14a.

The district court referred petitioners’ motion to a magistrate judge, who recommended denying it. Pet. App. 66a-76a. The magistrate judge reasoned that the inclusion of overbroad language was “academic,” so long as the government’s “application of the order” had complied with Title III. *Id.* at 72a-73a. “In the case at bar,” he observed, “although the wiretap order *permitted* interception outside this court’s jurisdiction, the government did not actually intercept cellular communications outside this court’s jurisdiction” that it sought to introduce at trial. *Ibid.* The magistrate judge

accordingly recommended concluding that the orders were not “invalid on their face.” *Id.* at 73a.

The magistrate judge further recommended that, if the district court were to find the orders facially insufficient, it should still deny the motion to suppress because the overbroad language was “surplusage and did not implicate Congress’s core concerns in passing Title III.” Pet. App. 73a; see *id.* at 74a (citing *United States v. Radcliff*, 331 F.3d 1153, 1162 (10th Cir.), cert. denied, 540 U.S. 973 (2003)). The magistrate judge explained that Title III’s territoriality provision “does not directly and substantially implement the intent of Congress in enacting Title III,” because it “does not implicate Congress’s concerns for privacy and preventing the government’s unauthorized use of surveillance techniques.” *Id.* at 75a-76a.

The district court adopted the magistrate judge’s report and recommendation, explaining that the magistrate judge had found that, “as applied, the orders did not violate the statute” because “the government did not actually intercept cellular communications outside this Court’s jurisdiction.” Pet. App. 64a. After a jury trial, petitioners Los Dahda and Roosevelt Dahda were convicted on 15 counts and ten counts, and sentenced to 189 months of imprisonment and 201 months of imprisonment, respectively.

4. The court of appeals affirmed in relevant part. Pet. App. 1a-58a. It rejected petitioner Los Dahda’s challenge to the denial of the suppression motion, *id.* at 15a-25a, and applied that conclusion in petitioner Roosevelt Dahda’s case, *id.* at 39a-40a.

The court of appeals agreed with petitioners that the orders’ territoriality language reached beyond Title III’s limitations, because that language permitted

interception outside Kansas even when the government was not using an interception device that was itself mobile. Pet. App. 15a-20a (disagreeing with *Ramirez*). The court then stated, without any additional analysis, that “[t]hus, the orders were facially insufficient under Title III.” *Id.* at 20a.

The court of appeals determined, however, that “the facial defects” in the orders “did not require suppression.” Pet. App. 25a. The court explained that, under this Court’s approach in *Giordano, supra*, the orders did not violate one of “those statutory requirements that directly and substantially implement[s] the congressional intention to limit the use of intercept procedures to those situations clearly calling for the employment of this extraordinary investigative device.” *Id.* at 21a (quoting *Giordano*, 416 U.S. at 527) (brackets in original); see *ibid.* (relying on *Radcliff* to use this test when deciding whether to suppress for facial insufficiency under 18 U.S.C. 2518(10)(a)(ii)).

The court of appeals observed that “Congress’s goals for Title III” included “protection of the privacy of oral and wire communications” and “establishment of a uniform basis for authorizing the interception of oral and wire communications.” Pet. App. 22a. But it found that the territoriality provisions furthered neither goal. *Ibid.* The court explained that Title III’s privacy protections focus on “[l]imiting who can conduct wiretaps” and “creating an evidentiary burden for a wiretap (probable cause).” *Ibid.* The court reasoned that Title III’s territoriality provisions do neither of those things. *Ibid.* The court explained that they “potentially undermine uniformity by requiring prosecutors in multiple jurisdictions to coordinate about how they use electronic surveillance.” *Id.* at 23a. And the court rejected

petitioners' argument "that the territorial limitation thwarts forum shopping," reasoning that even under petitioners' interpretation, "the government can forum shop by using a listening post in the preferred judge's district," and that "law enforcement has free rein on where to put the listening post." *Id.* at 23a-24a.

SUMMARY OF ARGUMENT

The court of appeals correctly refused to require the suppression of the wiretapped communications introduced in petitioners' trial, which the government lawfully intercepted in Kansas in conformity with orders of the Kansas district court and Title III's territoriality provisions. Contrary to petitioners' contentions, Title III does not require the suppression of evidence intercepted in conformity with its substantive requirements, simply because the order authorizing that interception was overbroad, in that it mistakenly purported to authorize interception in some circumstances outside the issuing court's territorial jurisdiction. Petitioners press an extreme rule under which any error in a Title III order, of any nature or magnitude, automatically mandates suppression of any and all evidence intercepted under that order, including evidence wholly unaffected by the error. That rule is flawed in multiple respects.

A. As a threshold matter, although the court of appeals described the orders here as "facially insufficient," Pet. App. 20a, its judgment can and should be affirmed on the ground that an otherwise sufficient Title III order is not "insufficient on its face," 18 U.S.C. 2518(10)(a)(ii), when it also includes language that is overbroad in part. "Insufficient" means lacking something necessary, and the orders here were not missing anything at all. It is undisputed that the orders included all of the information Title III required them to

contain. See 18 U.S.C. 2518(4). The addition of overbroad language about how the government may intercept cellphone communications outside the court's territorial jurisdiction does not detract from the court's power to authorize interceptions in Kansas in full compliance with Title III's substantive requirements.

B. Even if an overbroad order could be characterized as "insufficient," the mistake in the orders here did not render them "insufficient on [their] face" for purposes of suppression under 18 U.S.C. 2518(10)(a)(ii). This Court has held that a communication is "unlawfully intercepted" for purposes of suppression under the neighboring subparagraph, 18 U.S.C. 2518(10)(a)(i), only when the interception has transgressed one of "those statutory requirements that directly and substantially implement[s] the congressional intention to limit the use of intercept procedures to those situations clearly calling for the employment of this extraordinary investigative device." *United States v. Giordano*, 416 U.S. 505, 527 (1974). A similar construction should apply in determining whether an order is "insufficient on its face," a phrase Congress could not have intended to incorporate every possible technical defect that an order might exhibit.

The overbroad language here did not intrude upon any "limit [on] the *use* of intercept procedures," *Giordano*, 416 U.S. at 527 (emphasis added). Title III does not require orders to address territoriality at all, and nothing in the territoriality language here detracts from the issuing court's clear and express intent to authorize interception over the listed phones to the full extent of its authority, which includes allowing interception in Kansas. Title III's territoriality limitations also do not meaningfully protect personal privacy, because

they address only *where*, not *whether*, interception will occur. It is undisputed that the government can intercept communications over a lawfully tapped mobile phone, regardless of where the target brings it, so long as the government listens from a wire room inside the jurisdiction of the court that issued the order.

Moreover, the issuing court's error here does not even affect whether interception can lawfully occur outside the court's territorial jurisdiction. Title III expressly allows the government to intercept communications outside the court's territorial jurisdiction, so long as it uses a "mobile interception device." 18 U.S.C. 2518(3). The issuing court apparently understood that provision to permit the government to intercept at a post outside of Kansas when the phone was also outside Kansas, based on existing but ultimately incorrect case law holding that a tapped cellphone is itself a "mobile interception device." See *United States v. Ramirez*, 112 F.3d 849 (7th Cir.), cert. denied, 522 U.S. 892 (1997). But that is merely a mistake of statutory interpretation about the circumstances in which the government may conduct interception outside the court's jurisdiction, as Title III itself expressly allows. It has no effect on *which* communications the government could intercept, and thus has no effect on personal privacy.

C. In any event, suppression is unwarranted because all of the evidence introduced at trial in this case was lawfully intercepted inside Kansas in compliance with Title III's territoriality provisions. Title III does not require courts to suppress all evidence when an order is "insufficient on its face" in only some of its applications and those applications are not relevant to the evidence to be used at trial. Congress designed Title III's suppression remedy for statutory violations to be no

broader than the exclusionary rule for constitutional violations. And following this Court’s guidance, the courts of appeals have uniformly concluded that when a warrant is invalid in only some of its applications, suppression should extend only to evidence that results from that defect—not to evidence that was lawfully obtained under valid applications of the same warrant. Nothing in Title III suggests application of a broader rule, under which courts would be required to exclude probative evidence of guilt whose interception was not the result of any statutory or constitutional error.

ARGUMENT

All of the wiretapped communications the government introduced at trial here were intercepted in Kansas pursuant to orders of the Kansas district court authorizing such interception to occur. It is accordingly undisputed that all of that evidence was lawfully intercepted in conformity with Title III and its territoriality provisions. In urging that this evidence nonetheless should be suppressed, petitioners take the extreme view that (1) an otherwise sufficient order that also includes overbroad language can be deemed “insufficient on its face” to authorize interception, 18 U.S.C. 2518(10)(a)(ii), see Pet. Br. 22; (2) any error in an order, no matter how minor, renders the order per se “insufficient on its face,” *ibid.*; and (3) an error that renders an order “insufficient” for purposes of some interceptions requires suppression of all interceptions, see Pet. Br. 23. None of those propositions is correct—let alone all of them.

A. The Title III Orders In This Case Were Overbroad, Not “Insufficient”

Title III’s text makes clear that the orders here, which included everything necessary for the government to intercept communications, were not “*insufficient* on [their] face” simply because they *also* included an unnecessary paragraph reflecting a mistaken interpretation of the circumstances in which Title III permits interception outside Kansas. Although the court of appeals, without analysis, accepted the proposition that this overbreadth made these orders insufficient, Pet. App. 20a, the government has consistently maintained otherwise, including at the certiorari stage in this Court. See Br. in Opp. 21-22. That issue is logically antecedent to the question presented, necessary to its consideration, and dispositive of this case. See *United States v. Grubbs*, 547 U.S. 90, 94 & n.1 (2006) (resolving “antecedent” issue necessary to “an intelligent resolution of the question presented”) (citation omitted); Pet. Br. 21-23 (addressing insufficiency issue).

1. As petitioners recognize, “[b]ecause Title III does not define the phrase ‘insufficient on its face,’ the Court should ‘look first to the [phrase’s] ordinary meaning.’” Pet. Br. 22 (quoting *Schindler Elevator Corp. v. United States ex rel. Kirk*, 563 U.S. 401, 407 (2011)) (brackets in original). Both at the time of Title III’s passage and today, the word “insufficient” has ordinarily meant “[d]eficient in force, quality, or amount; lacking in what is necessary or requisite; inadequate.” 5 *Oxford English Dictionary* 359 (1933); see *Webster’s Third New International Dictionary* 1172 (2002) (*Webster’s Third*) (“inadequate to some implied or designated need, use, or purpose”); *Webster’s New International Dictionary*

1288 (2d ed. 1958) (similar). An order thus is “insufficient on its face” if its face shows that it is lacking something necessary to allow the government to rely on that order to conduct interception.

The orders here are not “insufficient” to authorize interception, because they are not missing anything that the statute requires. Title III defines, in 18 U.S.C. 2518(4), the information that an order must contain in order for it to authorize interception. To authorize interception over a cellphone, an order “shall specify,” among other things, the target’s identity, cellphone number or other unique identifier, the suspected offense, the type of communications sought to be intercepted, and the period in which interception is permitted. *Ibid.*; see S. Rep. No. 1097, 90th Cong., 2d Sess. 102 (1968) (Senate Report) (“Subparagraph (4) sets out * * * the requirements that each order authorizing or approving the interception of wire or oral communications must meet.”). It is undisputed that the orders here contain all of the necessary information. See J.A. 93-178 (reproducing orders).

Section 2518(4) does not require an order to say anything about the places where interception over a cellphone is authorized. Rather, the statute itself provides territoriality rules that every order incorporates by default and need not repeat: A court “may enter” an order “authorizing or approving interception * * * within the territorial jurisdiction of the court in which the judge is sitting (and outside that jurisdiction but within the United States in the case of a mobile interception device authorized by a Federal court within such jurisdiction).” 18 U.S.C. 2518(3). In contrast to the sort of information that each order is required to contain—such as the official who approved the application, the phones

to be targeted, or the duration of interception—that territorial scope is inherent and is not presumed to vary in each case.

2. Petitioners do not dispute that the Title III orders in this case would be sufficient if the paragraph on territoriality did not appear at all. The court’s addition of language restating the territorial limitations inherent in the statute, as the court understood them, did not make the orders “insufficient.” Adding *more* usually does not give an order *less* of something necessary, so as to render it “insufficient.” To the extent such a scenario might arise, it would be limited to situations in which the addition itself illustrates that something necessary is missing. Cf. *United States v. Leon*, 468 U.S. 897, 923 (1984) (“[D]epending on the circumstances of the particular case, a warrant may be so facially deficient—*i.e.*, in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid.”); see also *Groh v. Ramirez*, 540 U.S. 551, 558 (2004) (similar).

This case, however, presents no such circumstance. Nothing on the face of the orders here marked them as “insufficient” to confer upon law enforcement the full interception authority that Title III allows. An officer would be notified of the various case-specific determinations that the issuing court was required to make to authorize interception—*e.g.*, what phones would be tapped, how long interception could last. It is undisputed that those determinations here satisfied Title III and the constitutional requirement of particularization. And an officer executing the order would have no reason to believe that the issuing court had failed to take one of the steps necessary to approve interception. Indeed, it is undisputed that the court here did, in fact, take each

of the necessary steps and thus authorized interception to the full extent of Title III's territorial scope. Its orders were in no way "insufficient."

B. Suppression Is Unwarranted Because The Mistake In The Orders Is Not A Fundamental Defect

Even assuming that some overbroad orders could be considered "insufficient on [their] face," the orders here should not be. Only a defect that renders an order so deficient on its face that the government cannot rely on it to intercept communications can render an order "insufficient on its face" for purposes of the suppression remedy. The colorable mistake of statutory interpretation reflected in these orders does not rise to that level.

1. Title III requires suppression for facial errors only when they are sufficiently fundamental to prevent the government from relying on the order to conduct interception

The suppression remedy in 18 U.S.C. 2518(10)(a) provides that a defendant "may move to suppress the contents of any wire or oral communication intercepted pursuant to this chapter, or evidence derived therefrom," on the grounds that (i) "the communication was unlawfully intercepted"; (ii) "the order of authorization or approval under which it was intercepted is insufficient on its face"; or (iii) "the interception was not made in conformity with the order of authorization or approval." *Ibid.* This Court's decisions addressing that provision illustrate that its terms should not be construed so broadly as to require suppression for every conceivable defect.

a. In the companion cases of *United States v. Giordano*, 416 U.S. 505 (1974), and *United States v. Chavez*, 416 U.S. 562 (1974), the Court distinguished two

types of Title III violations upon which the defendants in those cases had moved to suppress communications as “unlawfully intercepted” under subparagraph (i). In *Giordano*, the Court held that suppression was required when an improper official (the Attorney General’s executive assistant) had approved the government’s application for a Title III order. 416 U.S. at 508-509. In *Chavez*, by contrast, the Court held that suppression was *not* required when the government’s application had been approved by a proper official, but it incorrectly identified a different official as the approver. 416 U.S. at 570.

In distinguishing the cases, the Court explained that a statutory violation renders a communication “unlawfully intercepted” for purposes of suppression under 18 U.S.C. 2518(10)(a)(i) only if its interception conflicts 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; *Chavez*, 416 U.S. at 575 (same). The Court found in *Giordano* that Title III’s requirement that wiretap applications be authorized only by certain officials “responsive to the political process” was a “critical precondition” to any judicial order. 416 U.S. at 516, 520. By contrast, the Court found in *Chavez* that Title III’s requirements that the authorizing official be *identified* in the wiretap application and order merely serve a “reporting function” and were not intended, “by themselves, to occupy a central, or even functional, role in guarding against unwarranted use” of wiretaps. 416 U.S. at 578-579.

The Court subsequently applied the same principles in *United States v. Donovan*, 429 U.S. 413 (1977), to

hold that suppression was not required based on a violation of Title III's requirements that the government identify "all those likely to be overheard" in applying for a wiretap and later inform the court "of all identifiable persons whose conversations were intercepted" under an order that the court issued. *Id.* at 435, 438; see *id.* at 434-439; see also 18 U.S.C. 2518(1)(b)(iv) and (8)(d). The Court explained that "[i]n no meaningful sense can it be said that the presence of that information as to additional targets would have precluded judicial authorization of the intercept." 429 U.S. at 436.

Although *Donovan*, *Giordano*, and *Chavez* focused on whether a communication was "unlawfully intercepted" so as to warrant suppression under 18 U.S.C. 2518(10)(a)(i), their limiting construction also informs whether an order is "insufficient on its face," so as to warrant suppression under 18 U.S.C. 2518(10)(a)(ii). Given this Court's construction of subparagraph (i) to reach only statutory violations that are sufficiently important to warrant suppression, it would be incongruous to construe suppression under neighboring subparagraph (ii) as mandatory for any facial error in the order, irrespective of its effect, nature, or magnitude. *Chavez* and *Donovan* illustrate that Congress countenanced the admission of at least some evidence that was *actually* intercepted in violation of Title III's statutory requirements. It is unlikely that Congress in its next breath enacted a provision so broad as to require suppression in every circumstance, no matter what—even of evidence that was lawfully intercepted within the issuing court's territorial jurisdiction. Rather, the two subparagraphs are naturally interpreted together to require suppression only for a limited category of errors

that are sufficiently serious to justify the extreme costs of suppression.

Accordingly, when a court is tasked with determining whether a defect apparent on the face of an order renders it “insufficient” notwithstanding that Congress did not itself make that information a prerequisite to conducting interception, see 18 U.S.C. 2518(4), a court must look to the nature and severity of the statutory violation in relation to the purpose of Title III’s suppression remedy. As a prerequisite to such an extreme sanction, the court must, as this Court did in *Giordano*, examine whether the statutory requirement that was violated “directly and substantially implement[s] 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.

b. Petitioners object (Br. 16) to relying on the *Giordano* test in construing suppression for facial insufficiency under subparagraph (ii). In their view, only subparagraph (i) is limited to fundamental defects, while subparagraph (ii) sets forth a blanket rule of suppression applicable whenever any defect of any sort is apparent on an order’s face. But for the reasons set forth above, that view is mistaken as a matter of the statutory text and context: The statute says “insufficient on its face,” 18 U.S.C. 2518(10)(a)(ii), not “imperfect on its face” or “invalid on its face in any respect.” Petitioners’ view would also lead to suppression in circumstances where it is pointless, and grant greater rights to defendants with claims of minor technical defects in the language of an order than to those with claims that evidence was actually intercepted in violation of Title III.

Petitioners err in their specific contention (Br. 16) that interpreting subparagraphs (i) and (ii) to contain the same overarching limitation would conflict with *Giordano*. The government argued in *Giordano* that, in order to avoid rendering the other subparagraphs of Section 2518(10)(a) surplusage, subparagraph (i)'s suppression remedy for “unlawfully intercepted” communications should apply only in the case of constitutional violations. 416 U.S. at 525-526. The Court considered that argument to have “substance,” but declined to adopt the government’s limiting construction. *Id.* at 527. The Court instead reasoned that no superfluity would exist under a construction of subparagraph (i) as applying only to violations of statutory requirements that “directly and substantially * * * limit the use of intercept procedures to those situations clearly calling for” such procedures. *Ibid.*

Contrary to petitioners’ assertion, taking those same considerations into account under subparagraph (ii) would not make that subparagraph superfluous. As a threshold matter, those considerations are relevant only in some (not all) subparagraph (ii) cases—namely, those in which a defendant claims that all of the evidence intercepted under an order must be suppressed due to some facial defect, notwithstanding that Congress did not itself make that information a prerequisite to conducting interception, see 18 U.S.C. 2518(4).

Subparagraph thus (ii) would still, for example, require suppression if the order and any accompanying materials entirely failed to identify the individual who approved the application, in violation of 18 U.S.C. 2518(1)(a) and (4)(d)—even if the application was actually approved by the Attorney General or other appro-

priate official and therefore suppression was not warranted under subparagraph (i). See *Giordano*, 416 U.S. at 525 n.14 (contrasting an “erroneous[]” identification of the official with the failure to identify the official); *United States v. Lomeli*, 676 F.3d 734, 742 (8th Cir. 2012) (affirming grant of motions to suppress where official not identified in order or its attachments). Suppression under subparagraph (ii), but not the other subparagraphs, would likewise be required if a judge issued an otherwise valid order but, before it was issued, a clerk mistakenly deleted the time limitations that the judge had intended to impose. Although the judge would have respected the relevant requirements of the statute, and ensuing interception would fit within the four corners of the order, the absence of a required limitation would nevertheless make the order “insufficient on its face” for purposes of suppression. See 18 U.S.C. 2518(4)(e) (an order “shall specify” the “period of time during which such interception is authorized”).

2. The legal mistake in the orders here did not prevent the government from relying on them to intercept communications over the tapped phones

The court of appeals conducted the correct inquiry, which it referred to as the “core concerns” inquiry, in affirming the denial of petitioners’ suppression motion here. Pet. App. 21a-25a. Although it did not locate the textual basis for its inquiry in the term “insufficient,” its analysis was nonetheless the same one that the text, as interpreted through the lens of this Court’s decisions, would require. See pp. 19-24, *supra*. And the court correctly recognized (Pet. App. 21a-25a) that the territorial language in the orders here does not require suppression.

The addition of that language to the orders here does not interfere with personal privacy because it is undisputed that the issuing court properly authorized interception to occur and the error did not expose any additional communications to the potential for government eavesdropping. All the same communications could be lawfully intercepted with or without the error. The language simply related to *where* government agents had to be located when intercepting those communications. Title III expressly authorizes interception outside a court’s territorial jurisdiction when the government uses a “mobile interception device.” 18 U.S.C. 2518(3). The court simply made a reasonable mistake of statutory interpretation in understanding the phrase, which Title III does not define. That mistake does not warrant suppression.

a. The territoriality language included in the orders here did not reflect the violation of any provision that “directly and substantially implement[s] 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. The language reflected the issuing court’s view—in accord with the Seventh Circuit, see *United States v. Ramirez*, 112 F.3d 849, 853, cert. denied, 522 U.S. 892 (1997)—that Title III permitted interception to occur wholly outside Kansas because a tapped mobile phone is a “mobile interception device.” The government defended that position below, but now acknowledges that the position—which the court of appeals rejected for the first time in this case, see Pet. App. 18a-20a—is incorrect. But the validity of that interpretation in the Tenth Circuit was an open ques-

tion at the time the orders were issued and the interception here occurred. *Ibid.* The issuing court’s legal mistake, on an unsettled issue of law about an undefined term in a statute, does not relate to whether interception was justified.

Indeed, the judge was willing to approve interception to the furthest reaches he viewed the law to allow. The government could and would have obtained an order authorizing the interception of all the wiretap evidence it introduced in this case irrespective of the judge’s error. As in *Donovan*, “[i]n no meaningful sense can it be said that the presence of [additional] information”—here, the correct interpretation of the statute—“would have precluded judicial authorization of the intercept,” 429 U.S. at 436.

b. Even if the error here were viewed to implicate the substantive territorial limitations of Title III, rather than simply the language in a judicial wiretap order, it would still have no bearing on whether the circumstances of the case “clearly call[ed] for the employment” of interception. *Giordano*, 416 U.S. at 527.

Title III’s territoriality provisions do not give any individual any meaningful protection for personal privacy. It is undisputed that, once a court issues an order authorizing interception, the government can lawfully intercept all the communications over the target mobile phone—regardless of where the target takes it—so long as the government’s listening post is located within the court’s territorial jurisdiction. Pet. App. 23a-24a. Title III’s territoriality provisions thus do not protect any of the target’s communications from the potential for lawful interception. While a target is likely to care *whether* government agents are listening to his communications,

he is unlikely to care much if at all about *where* the government agents are sitting when they do so.

Moreover, Title III's territoriality restrictions do not even require the intercepting government agents always to be sitting inside the court's territorial jurisdiction in order to intercept communications outside that area. Title III allows the government to intercept such communications when both the phone *and* the government's listening post are outside the court's jurisdiction, so long as the government uses a "mobile interception device." 18 U.S.C. 2518(3). In practice, the government no longer uses mobile interception devices to intercept cellphone communications. See p. 6 n.2, *supra*. But the orders here lawfully authorized the government to do so, and thus to intercept the same communications from outside the court's territorial jurisdiction. And it is difficult to see how the orders here invaded privacy to a greater degree by allowing the government to intercept the same communications at a wire room in Missouri, rather than through using the more invasive means of installing some kind of interception device on the target phones themselves. Cf. *United States v. Jones*, 565 U.S. 400, 404-405 (2012) (relying on common-law trespass principles to hold that the Fourth Amendment requires a warrant for the physical installation of a GPS tracker on a car).

c. Petitioners contend (Br. 37-38) that, because "[i]t is axiomatic that a court may act only within its own jurisdiction," the issuing court here necessarily must have violated a core concern of the statute. The axiom is correct, but petitioners' corollary conclusion does not follow. Congress defines the jurisdiction of the lower federal courts through positive law. See U.S. Const. Art. III, § 1. And in Title III, Congress expressly allowed

district courts to authorize the government to intercept communications outside the court's territorial jurisdiction, if the government uses a "mobile interception device." 18 U.S.C. 2518(3). The orders here omitted that last qualifier (that the government must use a mobile interception device) apparently based on a misunderstanding that the tapped mobile phone itself qualified as a "mobile interception device." The issuing court's error here was thus not a violation of axiomatic jurisdictional principles, but a more mundane mistake of statutory interpretation on a contestable issue.

The principles of law applicable to *that* kind of error strongly disfavor suppression. In *United States v. Ojeda Rios*, 495 U.S. 257 (1990), this Court held that a mistake of statutory interpretation by the government that was "objectively reasonable at the time" did not require suppression—even under a different provision of Title III with an "explicit exclusionary remedy" mandating suppression whenever the government failed to comply with a statutory requirement to seal intercepted communications. *Id.* at 260, 266-267; see 18 U.S.C. 2518(8)(a) (compliance "shall be a prerequisite for the use or disclosure" of intercepted communications at trial). It would be anomalous to interpret the general Title III suppression remedy at issue here nonetheless to require suppression in similar circumstances.

More broadly, Title III's suppression remedy for interception conducted pursuant to an order that is "insufficient on its face" can readily be analogized to the suppression remedy for "facially deficient" warrants in the Fourth Amendment context, *Leon*, 468 U.S. at 923. And in that context, a search pursuant to a warrant issued in excess of the court's jurisdiction would gener-

ally not result in suppression “if the police acted ‘in objectively reasonable reliance’” on that warrant, *Herring v. United States*, 555 U.S. 135, 142 (2009) (quoting *Leon*, 468 U.S. at 922), or if the “heavy costs” of suppression “outweigh” its “deterrence benefits,” *Davis v. United States*, 564 U.S. 229, 237 (2011). Cf. *Herring*, 555 U.S. at 136-138 (no suppression following an arrest made in reasonable reliance on a police database showing an outstanding arrest warrant, where another police employee had negligently failed to update the database to show that the warrant no longer existed); *Arizona v. Evans*, 514 U.S. 1, 11-16 (1995) (similar, where mistaken judicial records failed to show that the warrant no longer existed).

Courts have treated mistakes about territoriality the same way, suppressing evidence when, among other things, the error was obvious and the officer should have known that the warrant was issued in excess of the court’s jurisdiction, e.g., *United States v. Krueger*, 809 F.3d 1109, 1113 (10th Cir. 2015); see *id.* at 1126 (Gorsuch, J. concurring), but have declined to suppress evidence when the error was *not* obvious, and in particular when the question was unsettled, e.g., *United States v. Houston*, 665 F.3d 991, 996 (8th Cir.) (declining to impose “a duty on officers exercising a search warrant obtained without deceit” to know “the legal and jurisdictional limits of a judge’s power to issue interstate search warrants”), cert. denied, 566 U.S. 1004 (2012).⁴

⁴ The government has argued that violations of a statute or rule (rather than a constitutional provision) do not warrant suppression under the exclusionary rule. See *Sanchez-Llamas v. Oregon*, 548 U.S. 331, 348 (2006). Although Title III itself imposes a statutory suppression remedy, that principle counsels against pressing any

The government has long argued that Title III’s suppression remedy incorporates a good-faith exception. See *United States v. Malekzadeh*, 855 F.2d 1492, 1497 (11th Cir. 1988), cert. denied, 489 U.S. 1029 (1989). But whether or not it does, see *United States v. Barajas*, 710 F.3d 1102, 1110 & n.4 (10th Cir.) (noting circuit conflict on the good-faith issue), cert. denied, 134 S. Ct. 230 (2013), it is still difficult to see why Congress would have intended suppression in the circumstances here.

Petitioners provide no practical reason why Congress would have intended an error of the sort at issue here to require suppression. Petitioners suggest (Br. 36) that Congress intended Title III’s territoriality provisions to “restrict[] the ability of prosecutors to engage in forum shopping.” But the court of appeals correctly rejected that contention, because Title III’s limitations “do[] not prevent forum shopping” at all. Pet. App. 23a. Even under petitioners’ interpretation, it is undisputed that “the government can forum shop by using a listening post in the preferred judge’s district,” and “law enforcement has free rein on where to put the listening post.” *Id.* at 24a.

The mere characterization of an error as “jurisdictional” in nature also does not suggest that suppression is required. Cf. *Steel Co. v. Citizens for a Better Env’t*, 523 U.S. 83, 90 (1998) (noting that “[j]urisdiction’ * * * is a word of many, too many, meanings”) (citation omitted). The error here relates to what qualifies as a “mobile interception device” that the government may permissibly use to conduct electronic surveillance outside of the district, not to the bedrock authority of a court to act. Petitioners would presumably agree that the orders

suppression remedy beyond what Congress has unequivocally required.

here would have been sufficient had the issuing court mistakenly viewed the “jurisdictional” scope of its territorial authority too *narrowly*—say, by including in the orders a reading of the statute as altogether foreclosing interception when the tapped cellphone was outside of Kansas. It would be anomalous nonetheless to label the orders here, which the court clearly intended to reach as far as the statute allowed, as “insufficient” to authorize interception in Kansas consistent with Title III.

C. Any Insufficiency Arising From The Overbreadth Of The Orders In This Case Would Be Severable

Even if the overbroad language rendered the orders here “insufficient on [their] face” in some applications, it would not render them “insufficient on [their] face” in all of them. Rather, the communications used at trial here were intercepted in Kansas pursuant to valid applications of the orders and are readily severable from any potential invalid applications. And Title III does not require suppression of evidence that—like the evidence at issue here—was intercepted without reliance on any legal error that an order might contain. The government would have lawfully intercepted the same evidence it used at trial in the same place at the same time, with or without the erroneous paragraph in the orders. Suppression accordingly is unwarranted. See Pet. App. 72a (concluding that any overbreadth was “academic” to the admissibility of the evidence intercepted in Kansas and used at trial).

1. Nothing in Title III suggests that Congress intended to enact a blanket suppression remedy that would dispense with traditional fruit-of-the-poisonous-tree analysis. To the contrary, Congress focused the admissibility inquiry on the propriety of disclosing the actual evidence used at trial, not on hypothetical issues

that might have arisen if the government had sought to use different evidence at trial.

The statute provides that, when wire or oral communications have been intercepted, “no *part* of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial” if “the disclosure *of that information* would be in violation of this chapter.” 18 U.S.C. 2515 (emphases added). Similarly, subparagraphs (i) and (iii) of Section 2518(10)(a) permit a motion “to suppress the contents of any wire or oral communication intercepted pursuant to this chapter, or evidence derived therefrom,” when “*the communication* was unlawfully intercepted” or “*the interception* was not made in conformity with the order of authorization or approval.” 18 U.S.C. 2518(10)(a)(i) and (iii) (emphases added).

Subparagraph (ii), in turn, authorizes suppression only when “the order of authorization or approval under which” a communication was intercepted “is insufficient on its face.” 18 U.S.C. 2518(10)(a)(ii). An order can be “insufficient”—*i.e.*, “inadequate to *some* implied or designated need, use, or purpose”—without being “inadequate to” *every* “implied or designated need, use, or purpose.” *Webster’s Third* 1172 (emphasis added). Had Congress intended a blanket suppression remedy that would apply to any evidence intercepted under any order that was deficient in any respect, regardless of the relationship between the deficiency and the evidence, it would have said so more clearly. And the Senate Report accompanying Title III’s enactment confirms that Title III’s suppression remedy was intended to deny the government only the “fruits of [its] unlawful actions.” Senate Report 69; see *Giordano*, 416 U.S. at 528-529 (looking to this report).

2. Congress had no intent “to press the scope of the suppression role beyond present search and seizure law.” Senate Report 96. And under both then-existing and current search and seizure law, suppression is not justified in the absence of a sufficient “causal relationship between the unconstitutional act and the discovery of evidence.” *Utah v. Strieff*, 136 S. Ct. 2056, 2061 (2016). For example, under the “independent source” doctrine, courts may “admit evidence obtained in an unlawful search if officers independently acquired it from a separate, independent source.” *Ibid.* (citing *Murray v. United States*, 487 U.S. 533, 537 (1988)). Under the “inevitable discovery” doctrine, courts may admit “evidence that would have been discovered even without the unconstitutional source.” *Ibid.* (citing *Nix v. Williams*, 467 U.S. 431, 443-444 (1984)). And under the “attenuation doctrine,” courts may admit evidence “when the connection between unconstitutional police conduct and the evidence is remote or has been interrupted by some intervening circumstance,” such that suppression is no longer warranted. *Ibid.*; see *Wong Sun v. United States*, 371 U.S. 471 (1963); see also Senate Report 96 (stating that Congress had “no intention to change the attenuation rule” when it enacted Title III).

Both before and after Congress enacted Title III, the lower courts have recognized “severance”—also known as “partial invalidity,” “partial suppression,” or “redaction”—as an additional application of similar causation principles. See *United States v. Sells*, 463 F.3d 1148, 1150 n.1 (10th Cir. 2006) (collecting cases from every circuit), cert. denied, 549 U.S. 1229 (2007); 2 Wayne R. LaFare, *Search and Seizure: A Treatise on the Fourth Amendment* § 4.6(f) (5th ed. 2012) (LaFare). Under that doctrine, when a traditional

search warrant satisfies either the Fourth Amendment's particularity or probable cause requirements only in part, courts need not suppress *all* the evidence obtained pursuant to the warrant. Rather, if the valid and invalid applications can be severed, courts may admit the evidence obtained under valid applications of the warrant, and suppress only the evidence "seized under the authority" of the parts that are invalid. *United States v. Christine*, 687 F.2d 749, 754 (3d Cir. 1982); *Aday v. Superior Court*, 362 P.2d 47, 52 (Cal. 1961); LaFave § 4.6(f), at 814-815 (describing *Aday* as the "leading case" and stating that its rule "is sound"); cf. *Waller v. Georgia*, 467 U.S. 39, 43 n.3 (1984) (rejecting suppression remedy for validly seized items where police also made invalid seizures in warrant-authorized search).⁵ For example, if a warrant authorizes the search of two apartments, but probable cause was lacking as to one, any suppression remedy would be limited to that apartment. See, e.g., *United States v. Pitts*, 173 F.3d 677, 679-681 (8th Cir. 1999).

The severance doctrine's underlying rationale is that "it would be harsh medicine indeed if a warrant issued on probable cause and particularly describing certain items were to be invalidated in toto merely because the affiant and magistrate erred in seeking and permitting a search for other items as well." LaFave § 4.6(f), at 815. And that rationale translates with full force to

⁵ Courts acknowledge that severability might be inappropriate where officers "abuse * * * the warrant procedure" by obtaining a warrant "essentially general in character" that nevertheless "meet[s] the requirement of particularity" in respect to certain "minor items." LaFave § 4.6(f), at 814 (quoting *Aday*, 362 P.2d at 52). Here, however, the orders satisfied all particularity requirements and were capable of myriad valid applications.

Title III. When a defect in a Title III order (*e.g.*, the omission of a time limit for interception, see 18 U.S.C. 2518(4)(e)) renders it “insufficient on its face” in all of its applications (because it categorically lacks a necessary privacy-protecting judicial determination), then all evidence obtained pursuant to that order is the fruit of the violation and may potentially be suppressed.⁶ But if a defect causes an order to be “insufficient on its face” in only *some* of its applications and they can be severed, then only the evidence intercepted pursuant to the invalid applications would be subject to suppression, and the untainted evidence should be admitted into evidence. Cf. LaFave § 4.6(f), at 816 (“When [a] warrant’s fault is not so pervasive,” the objective of deterrence “may be served in the same way and to the same degree by limiting suppression to the fruits of the warrant’s unconstitutional component.”).

3. The “grave adverse consequence that exclusion of relevant incriminating evidence always entails,” *Hudson v. Michigan*, 547 U.S. 586, 595 (2006), makes it especially unlikely that Congress intended suppression of evidence when its interception lacked a causal connection to a statutory or constitutional violation. “Quite apart from the requirement of unattenuated causation, the exclusionary rule has never been applied except ‘where its deterrence benefits outweigh its substantial social costs.’” *Id.* at 594 (quoting *Pennsylvania Bd. of Prob. & Parole v. Scott*, 524 U.S. 357, 363 (1998)). Noth-

⁶ Even in the case of a facial invalidity, suppression might not be warranted if the officer acted in good faith reliance on the Title III order. See p. 30, *supra* (noting circuit conflict on this issue). The government did not rely on a good faith argument below and accordingly does not press one in this Court.

ing suggests that Congress intended Title III's suppression remedy, which was meant to mirror the Fourth Amendment's, see Senate Report 96, to apply in situations where it would serve no significant purpose.

This Court has explained that the constitutional suppression remedy is designed to "safeguard Fourth Amendment rights generally through its deterrent effect." *Leon*, 468 U.S. at 906 (quoting *United States v. Calandra*, 414 U.S. 338, 348 (1974)). Suppression is an "extreme sanction," *id.* at 916, that "always entails" significant societal costs, *Hudson*, 547 U.S. at 595. Most obviously, it can allow "guilty and possibly dangerous defendants [to] go free—something that 'offends basic concepts of the criminal justice system.'" *Herring*, 555 U.S. at 141 (quoting *Leon*, 468 U.S. at 908). Accordingly, the Court has found suppression warranted only where its "remedial purpose" is "effectively advanced" and the benefits of deterrence outweigh suppression's "substantial social costs." *Illinois v. Krull*, 480 U.S. 340, 347, 352 (1987) (quoting *Leon*, 468 U.S. at 907).

Petitioners' all-or-nothing approach to suppression would contravene those fundamental principles by mandating suppression of evidence without a causal link to the underlying illegality, without an apparent justification, and where Title III already provides an adequate deterrent. For example, Congress provided that a wiretap order must identify the target phones. See 18 U.S.C. 2518(4)(b); p. 5 n.1, *supra*. If a court issued an otherwise valid order that properly identified ten cellphones to be tapped, but also purported to authorize interception over an eleventh cellphone ("target phone 11") without giving a phone number or other unique identifier at all, the order would be "insufficient on its face" to support interception from the unidentified line,

18 U.S.C. 2518(10)(a)(ii). But in the absence of severance, a court would be required to suppress evidence intercepted not only over the unidentified cellphone, but also over all the properly identified phones mentioned in the same order—notwithstanding that the order was sufficient to authorize interception over those ten lines and that interception was entirely lawful.

Similarly, Congress provided that interception cannot last more than 30 days, starting from the earlier of the day interception begins or the expiration of a 10-day grace period after the order is entered. 18 U.S.C. 2518(5). Accordingly, interception always must end by day 40 (the 10-day grace period plus 30 days). If a court authorized interception for 30 days beginning from the date interceptions commence but omitted the requirement that the clock automatically start after 10 days, and the government did not begin interception until day 15, then the government of course could not use evidence intercepted from days 41 through 45: Under Title III's plain terms, the order would have already expired. *Ibid.* In the absence of severance, however, a court also would be required to suppress evidence intercepted from days 15 through 40—notwithstanding that the order on its face validly authorized that interception. Nothing in Title III mandates such a counterproductive result.

4. No decision of this Court or any court of appeals has adopted a “harsh medicine” rule under which any insufficiency in a Title III order would automatically require suppression of all evidence intercepted under it.

The only decision in which this Court has required suppression of Title III evidence was *Giordano*. But *Giordano*'s conclusion that “suppression must follow” when evidence used at trial was *in fact* “unlawfully

intercepted” within the meaning of 18 U.S.C. 2518(10)(a)(i), 416 U.S. at 528, does not aid petitioners here. The statutory error at issue in *Giordano* was an overarching one that tainted all of the evidence the government had intercepted—namely, that no appropriate official in the Executive Branch had approved the government’s application for the Title III order that had authorized the interceptions that the government sought to introduce. See *id.* at 508-509. The Court did not suggest that, in circumstances in which a statutory violation tainted the interception of only *some* evidence, Title III would require suppression of untainted evidence as well.

Every court of appeals that has considered the issue has rejected a rule that would require suppression of lawfully intercepted evidence whenever any kind of defect whatsoever is apparent on the face of an order, without regard to its significance or bearing on interception of the evidence at issue. See *United States v. Moore*, 41 F.3d 370, 374 (8th Cir. 1994) (“[E]very circuit to consider the question has held that § 2518(10)(a)(ii) does not require suppression if the facial insufficiency of the wiretap order is no more than a technical defect.”); see also *United States v. Radcliff*, 331 F.3d 1153, 1155 (10th Cir.) (no suppression when “merely a technical defect”), cert. denied, 540 U.S. 973 (2003); *United States v. Cunningham*, 113 F.3d 289, 293-294 (1st Cir.) (no suppression of order “identif[ying] place and type” of communications to be intercepted “in a confusing language,” where “the judge and the executing officer knew what had [actually] been proposed and authorized”), cert. denied, 522 U.S. 862 (1997); *United States v. Holden*, 603 Fed. Appx. 744, 749 (11th Cir.) (per curiam) (“[F]acial insufficiency * * * that amounts to a

mere technical defect need not result in suppression.”), cert. denied, 136 S. Ct. 522 (2015), and 136 S. Ct. 851 (2016). Furthermore, as noted above, every circuit follows the severance doctrine in the Fourth Amendment context. See *Sells*, 463 F.3d at 1150 n.1.

The one circuit decision on which petitioners rely, *United States v. Glover*, 736 F.3d 509 (D.C. Cir. 2013), likewise does not embrace petitioners’ sweeping and all-or-nothing approach. The court of appeals in *Glover* required suppression only of evidence that it concluded had actually been intercepted in violation of Title III. See *id.* at 513-515. And although the court stated that “subparagraph (ii) creates a ‘mechanical test’ under which ‘suppression is the mandatory remedy,’” Pet. Br. 23 (brackets omitted) (quoting *Glover*, 736 F.3d at 513), subsequent decisions have clarified that it “left open the possibility” that a “technical defect” in an interception order might not require suppression, *United States v. Scurry*, 821 F.3d 1, 12 (D.C. Cir. 2016) (citing *Glover*, 736 F.3d at 515). It thus recognized that some situations may exist in which a statutory violation is apparent on the face of an order but suppression is nonetheless inappropriate.

5. A case like this one, in which the defect in the order had no effect on the interception of the evidence introduced at trial, presents such a situation. The overbroad language in the orders here effectively treating a cellphone as a “mobile interception device” was neither a but-for nor a proximate cause of the government’s interception of the evidence used at trial. The issuing court here included in its orders all the information necessary to authorize interception; it simply added additional language reflecting a subtle mistake of statutory interpretation (effectively treating a tapped mobile

phone as a “mobile interception device”). The mistake was relevant in only some applications of the orders (when the cellphone was outside Kansas and the government was listening from outside Kansas). And even in that subset of applications, the mistake affected only how such interception could occur (without using an interception device that was itself mobile), not whether Title III could ever permit interception outside the court’s territorial jurisdiction. The government lawfully intercepted communications over 10 of the 11 target phones by listening from a wire room in Kansas, J.A. 46-47, and it avoided the potential difficulty with interceptions over the one remaining phone by not using any of that evidence at trial.

It is one thing to suppress evidence and potentially let the criminal “go free because the constable has blundered.” *People v. Defore*, 150 N.E. 585, 588-589 (N.Y.) (Cardozo, J.), cert. denied, 270 U.S. 657 (1926). But it would be quite another to suppress evidence and potentially let petitioners go free here. Suppression in these circumstances would serve no purpose, and neither general principles of law nor Title III require it.⁷

⁷ If the Court declines to affirm the court of appeals’ judgment, it should remand for further proceedings in which that court can address arguments that it did not previously need to reach. First, Section 2518(10)(a), by its terms, applies only to the interception of “wire or oral” communications, and some of the communications at issue (such as text messages, two of which were admitted at trial, see Gov’t Exs. 656, 756) are instead electronic communications. See 18 U.S.C. 2510(12). Second, as the government explained below, any error here was harmless because each petitioner’s guilt was established by overwhelming non-Title III evidence—including the testimony of cooperating witnesses, business records, and physical law-enforcement surveillance. See Fed. R. Crim. P. 52(a); 15-3236 Gov’t C.A. Br. 32-33; 15-3237 Gov’t C.A. Br. 33-34.

CONCLUSION

The judgment of the court of appeals should be affirmed.

Respectfully submitted.

NOEL J. FRANCISCO
Solicitor General

JOHN P. CRONAN
*Acting Assistant Attorney
General*

MICHAEL R. DREEBEN
Deputy Solicitor General

ERIC J. FEIGIN
ZACHARY D. TRIPP
*Assistants to the Solicitor
General*

FINNUALA K. TESSIER
Attorney

JANUARY 2018

APPENDIX

1. 18 U.S.C. 2510 provides:

Definitions

As used in this chapter—

(1) “wire communication” means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce;

(2) “oral communication” means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication;

(3) “State” means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States;

(4) “intercept” means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.¹

¹ So in original. The period probably should be a semicolon.

(5) “electronic, mechanical, or other device” means any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than—

(a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or (ii) being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties;

(b) a hearing aid or similar device being used to correct subnormal hearing to not better than normal;

(6) “person” means any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation;

(7) “Investigative or law enforcement officer” means any officer of the United States or of a State or political subdivision thereof, who is empowered by law to conduct investigations of or to make arrests for offenses enumerated in this chapter, and any attorney authorized by law to prosecute or participate in the prosecution of such offenses;

(8) “contents”, when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication;

(9) “Judge of competent jurisdiction” means—

(a) a judge of a United States district court or a United States court of appeals; and

(b) a judge of any court of general criminal jurisdiction of a State who is authorized by a statute of that State to enter orders authorizing interceptions of wire, oral, or electronic communications;

(10) “communication common carrier” has the meaning given that term in section 3 of the Communications Act of 1934;

(11) “aggrieved person” means a person who was a party to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed;

(12) “electronic communication” means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—

(A) any wire or oral communication;

(B) any communication made through a tone-only paging device;

(C) any communication from a tracking device (as defined in section 3117 of this title); or

(D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds;

(13) “user” means any person or entity who—

(A) uses an electronic communication service; and

(B) is duly authorized by the provider of such service to engage in such use;

(14) “electronic communications system” means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications;

(15) “electronic communication service” means any service which provides to users thereof the ability to send or receive wire or electronic communications;

(16) “readily accessible to the general public” means, with respect to a radio communication, that such communication is not—

(A) scrambled or encrypted;

(B) transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication;

(C) carried on a subcarrier or other signal subsidiary to a radio transmission;

(D) transmitted over a communication system provided by a common carrier, unless the communication is a tone only paging system communication; or

(E) transmitted on frequencies allocated under part 25, subpart D, E, or F of part 74, or part 94 of the Rules of the Federal Communications Commission, unless, in the case of a communication transmitted on a frequency allocated under part 74 that is not exclusively allocated to broadcast auxiliary services, the communication is a two-way voice communication by radio;

(17) “electronic storage” means—

(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication;

(18) “aural transfer” means a transfer containing the human voice at any point between and including the point of origin and the point of reception;

(19) “foreign intelligence information”, for purposes of section 2517(6) of this title, means—

(A) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against—

(i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

6a

(ii) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

(iii) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(B) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to—

(i) the national defense or the security of the United States; or

(ii) the conduct of the foreign affairs of the United States;

(20) “protected computer” has the meaning set forth in section 1030; and

(21) “computer trespasser”—

(A) means a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer; and

(B) does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer.

2. 18 U.S.C. 2515 provides:

Prohibition of use as evidence of intercepted wire or oral communications

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 this chapter.

3. 18 U.S.C. 2516 (2012 & Supp. IV 2016) provides:

Authorization for interception of wire, oral, or electronic communications

(1) The Attorney General, Deputy Attorney General, Associate Attorney General,¹ or any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General or acting Deputy Assistant Attorney General in the Criminal Division or National Security Division specially designated by the Attorney General, may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant in conformity with section 2518 of this chapter an order authorizing or approving the interception of wire or oral communications by the Federal Bureau of Investigation, or a Federal agency having responsibility for the investigation of the offense as

¹ See 1984 Amendment note below.

to which the application is made, when such interception may provide or has provided evidence of—

(a) any offense punishable by death or by imprisonment for more than one year under sections 2122 and 2274 through 2277 of title 42 of the United States Code (relating to the enforcement of the Atomic Energy Act of 1954), section 2284 of title 42 of the United States Code (relating to sabotage of nuclear facilities or fuel), or under the following chapters of this title: chapter 10 (relating to biological weapons), chapter 37 (relating to espionage), chapter 55 (relating to kidnapping), chapter 90 (relating to protection of trade secrets), chapter 105 (relating to sabotage), chapter 115 (relating to treason), chapter 102 (relating to riots), chapter 65 (relating to malicious mischief), chapter 111 (relating to destruction of vessels), or chapter 81 (relating to piracy);

(b) a violation of section 186 or section 501(c) of title 29, United States Code (dealing with restrictions on payments and loans to labor organizations), or any offense which involves murder, kidnapping, robbery, or extortion, and which is punishable under this title;

(c) any offense which is punishable under the following sections of this title: section 37 (relating to violence at international airports), section 43 (relating to animal enterprise terrorism), section 81 (arson within special maritime and territorial jurisdiction), section 201 (bribery of public officials and witnesses), section 215 (relating to bribery of bank officials), section 224 (bribery in sporting contests), subsection (d), (e), (f), (g), (h), or (i) of section 844 (unlawful use of explosives), section 1032 (relating to concealment of

assets), section 1084 (transmission of wagering information), section 751 (relating to escape), section 832 (relating to nuclear and weapons of mass destruction threats), section 842 (relating to explosive materials), section 930 (relating to possession of weapons in Federal facilities), section 1014 (relating to loans and credit applications generally; renewals and discounts), section 1114 (relating to officers and employees of the United States), section 1116 (relating to protection of foreign officials), sections 1503, 1512, and 1513 (influencing or injuring an officer, juror, or witness generally), section 1510 (obstruction of criminal investigations), section 1511 (obstruction of State or local law enforcement), section 1581 (peonage), section 1584 (involuntary servitude), section 1589 (forced labor), section 1590 (trafficking with respect to peonage, slavery, involuntary servitude, or forced labor), section 1591 (sex trafficking of children by force, fraud, or coercion), section 1592 (unlawful conduct with respect to documents in furtherance of trafficking, peonage, slavery, involuntary servitude, or forced labor), section 1751 (Presidential and Presidential staff assassination, kidnapping, and assault), section 1951 (interference with commerce by threats or violence), section 1952 (interstate and foreign travel or transportation in aid of racketeering enterprises), section 1958 (relating to use of interstate commerce facilities in the commission of murder for hire), section 1959 (relating to violent crimes in aid of racketeering activity), section 1954 (offer, acceptance, or solicitation to influence operations of employee benefit plan), section 1955 (prohibition of business enterprises of gambling), section 1956 (laundering of monetary instruments), section 1957 (relating to engaging in

monetary transactions in property derived from specified unlawful activity), section 659 (theft from interstate shipment), section 664 (embezzlement from pension and welfare funds), section 1343 (fraud by wire, radio, or television), section 1344 (relating to bank fraud), section 1992 (relating to terrorist attacks against mass transportation), sections 2251 and 2252 (sexual exploitation of children), section 2251A (selling or buying of children), section 2252A (relating to material constituting or containing child pornography), section 1466A (relating to child obscenity), section 2260 (production of sexually explicit depictions of a minor for importation into the United States), sections 2421, 2422, 2423, and 2425 (relating to transportation for illegal sexual activity and related crimes), sections 2312, 2313, 2314, and 2315 (interstate transportation of stolen property), section 2321 (relating to trafficking in certain motor vehicles or motor vehicle parts), section 2340A (relating to torture), section 1203 (relating to hostage taking), section 1029 (relating to fraud and related activity in connection with access devices), section 3146 (relating to penalty for failure to appear), section 3521(b)(3) (relating to witness relocation and assistance), section 32 (relating to destruction of aircraft or aircraft facilities), section 38 (relating to aircraft parts fraud), section 1963 (violations with respect to racketeer influenced and corrupt organizations), section 115 (relating to threatening or retaliating against a Federal official), section 1341 (relating to mail fraud), a felony violation of section 1030 (relating to computer fraud and abuse), section 351 (violations with respect to congressional, Cabinet, or Supreme Court assassinations, kidnapping, and assault), section 831 (relating

to prohibited transactions involving nuclear materials), section 33 (relating to destruction of motor vehicles or motor vehicle facilities), section 175 (relating to biological weapons), section 175c (relating to variola virus), section 956 (conspiracy to harm persons or property overseas), a felony violation of section 1028 (relating to production of false identification documentation), section 1425 (relating to the procurement of citizenship or nationalization unlawfully), section 1426 (relating to the reproduction of naturalization or citizenship papers), section 1427 (relating to the sale of naturalization or citizenship papers), section 1541 (relating to passport issuance without authority), section 1542 (relating to false statements in passport applications), section 1543 (relating to forgery or false use of passports), section 1544 (relating to misuse of passports), section 1546 (relating to fraud and misuse of visas, permits, and other documents), or section 555 (relating to construction or use of international border tunnels);

(d) any offense involving counterfeiting punishable under section 471, 472, or 473 of this title;

(e) any offense involving fraud connected with a case under title 11 or the manufacture, importation, receiving, concealment, buying, selling, or otherwise dealing in narcotic drugs, marihuana, or other dangerous drugs, punishable under any law of the United States;

(f) any offense including extortionate credit transactions under sections 892, 893, or 894 of this title;

(g) a violation of section 5322 of title 31, United States Code (dealing with the reporting of currency

transactions), or section 5324 of title 31, United States Code (relating to structuring transactions to evade reporting requirement prohibited);

(h) any felony violation of sections 2511 and 2512 (relating to interception and disclosure of certain communications and to certain intercepting devices) of this title;

(i) any felony violation of chapter 71 (relating to obscenity) of this title;

(j) any violation of section 60123(b) (relating to destruction of a natural gas pipeline), section 46502 (relating to aircraft piracy), the second sentence of section 46504 (relating to assault on a flight crew with dangerous weapon), or section 46505(b)(3) or (c) (relating to explosive or incendiary devices, or endangerment of human life, by means of weapons on aircraft) of title 49;

(k) any criminal violation of section 2778 of title 22 (relating to the Arms Export Control Act);

(l) the location of any fugitive from justice from an offense described in this section;

(m) a violation of section 274, 277, or 278 of the Immigration and Nationality Act (8 U.S.C. 1324, 1327, or 1328) (relating to the smuggling of aliens);

(n) any felony violation of sections 922 and 924 of title 18, United States Code (relating to firearms);

(o) any violation of section 5861 of the Internal Revenue Code of 1986 (relating to firearms);

(p) a felony violation of section 1028 (relating to production of false identification documents), section

1542 (relating to false statements in passport applications), section 1546 (relating to fraud and misuse of visas, permits, and other documents), section 1028A (relating to aggravated identity theft) of this title or a violation of section 274, 277, or 278 of the Immigration and Nationality Act (relating to the smuggling of aliens); or²

(q) any criminal violation of section 229 (relating to chemical weapons) or section 2332, 2332a, 2332b, 2332d, 2332f, 2332g, 2332h³ 2339, 2339A, 2339B, 2339C, or 2339D of this title (relating to terrorism);

(r) any criminal violation of section 1 (relating to illegal restraints of trade or commerce), 2 (relating to illegal monopolizing of trade or commerce), or 3 (relating to illegal restraints of trade or commerce in territories or the District of Columbia) of the Sherman Act (15 U.S.C. 1, 2, 3);

(s) any violation of section 670 (relating to theft of medical products); or

(t) any conspiracy to commit any offense described in any subparagraph of this paragraph.

(2) The principal prosecuting attorney of any State, or the principal prosecuting attorney of any political subdivision thereof, if such attorney is authorized by a statute of that State to make application to a State court judge of competent jurisdiction for an order authorizing or approving the interception of wire, oral, or electronic communications, may apply to such judge for, and such judge may grant in conformity with section 2518 of this

² So in original. The word “or” probably should not appear.

³ So in original. Probably should be followed by a comma.

chapter and with the applicable State statute an order authorizing, or approving the interception of wire, oral, or electronic communications by investigative or law enforcement officers having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of the commission of the offense of murder, kidnapping³ human trafficking, child sexual exploitation, child pornography production,⁴ gambling, robbery, bribery, extortion, or dealing in narcotic drugs, marihuana or other dangerous drugs, or other crime dangerous to life, limb, or property, and punishable by imprisonment for more than one year, designated in any applicable State statute authorizing such interception, or any conspiracy to commit any of the foregoing offenses.

(3) Any attorney for the Government (as such term is defined for the purposes of the Federal Rules of Criminal Procedure) may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant, in conformity with section 2518 of this title, an order authorizing or approving the interception of electronic communications by an investigative or law enforcement officer having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of any Federal felony.

³ So in original. Probably should be followed by a comma.

⁴ So in original.

4. 18 U.S.C. 2518 provides:

Procedure for interception of wire, oral, or electronic communications

(1) Each application for an order authorizing or approving the interception of a wire, oral, or electronic communication under this chapter shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant's authority to make such application. Each application shall include the following information:

(a) the identity of the investigative or law enforcement officer making the application, and the officer authorizing the application;

(b) a full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued, including (i) details as to the particular offense that has been, is being, or is about to be committed, (ii) except as provided in subsection (11), a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted, (iii) a particular description of the type of communications sought to be intercepted, (iv) the identity of the person, if known, committing the offense and whose communications are to be intercepted;

(c) a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) a statement of the period of time for which the interception is required to be maintained. If the

nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter;

(e) a full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any judge for authorization to intercept, or for approval of interceptions of, wire, oral, or electronic communications involving any of the same persons, facilities or places specified in the application, and the action taken by the judge on each such application; and

(f) where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results.

(2) The judge may require the applicant to furnish additional testimony or documentary evidence in support of the application.

(3) Upon such application the judge may enter an ex parte order, as requested or as modified, authorizing or approving interception of wire, oral, or electronic communications within the territorial jurisdiction of the court in which the judge is sitting (and outside that jurisdiction but within the United States in the case of a mobile interception device authorized by a Federal court within such jurisdiction), if the judge determines on the basis of the facts submitted by the applicant that—

(a) there is probable cause for belief that an individual is committing, has committed, or is about to

commit a particular offense enumerated in section 2516 of this chapter;

(b) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception;

(c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) except as provided in subsection (11), there is probable cause for belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person.

(4) Each order authorizing or approving the interception of any wire, oral, or electronic communication under this chapter shall specify—

(a) the identity of the person, if known, whose communications are to be intercepted;

(b) the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted;

(c) a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates;

(d) the identity of the agency authorized to intercept the communications, and of the person authorizing the application; and

(e) the period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained.

An order authorizing the interception of a wire, oral, or electronic communication under this chapter shall, upon request of the applicant, direct that a provider of wire or electronic communication service, landlord, custodian or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such service provider, landlord, custodian, or person is according the person whose communications are to be intercepted. Any provider of wire or electronic communication service, landlord, custodian or other person furnishing such facilities or technical assistance shall be compensated therefor by the applicant for reasonable expenses incurred in providing such facilities or assistance. Pursuant to section 2522 of this chapter, an order may also be issued to enforce the assistance capability and capacity requirements under the Communications Assistance for Law Enforcement Act.

(5) No order entered under this section may authorize or approve the interception of any wire, oral, or electronic communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days. Such thirty-day period begins on the earlier of the day on which the investigative or law enforcement officer first begins to conduct an interception under the order or ten days after the order is entered. Extensions of an order may be

granted, but only upon application for an extension made in accordance with subsection (1) of this section and the court making the findings required by subsection (3) of this section. The period of extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than thirty days. Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days. In the event the intercepted communication is in a code or foreign language, and an expert in that foreign language or code is not reasonably available during the interception period, minimization may be accomplished as soon as practicable after such interception. An interception under this chapter may be conducted in whole or in part by Government personnel, or by an individual operating under a contract with the Government, acting under the supervision of an investigative or law enforcement officer authorized to conduct the interception.

(6) Whenever an order authorizing interception is entered pursuant to this chapter, the order may require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. Such reports shall be made at such intervals as the judge may require.

(7) Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, who reasonably determines that—

(a) an emergency situation exists that involves—

(i) immediate danger of death or serious physical injury to any person,

(ii) conspiratorial activities threatening the national security interest, or

(iii) conspiratorial activities characteristic of organized crime,

that requires a wire, oral, or electronic communication to be intercepted before an order authorizing such interception can, with due diligence, be obtained, and

(b) there are grounds upon which an order could be entered under this chapter to authorize such interception,

may intercept such wire, oral, or electronic communication if an application for an order approving the interception is made in accordance with this section within forty-eight hours after the interception has occurred, or begins to occur. In the absence of an order, such interception shall immediately terminate when the communication sought is obtained or when the application for the order is denied, whichever is earlier. In the event such application for approval is denied, or in any other case where the interception is terminated without an order

having been issued, the contents of any wire, oral, or electronic communication intercepted shall be treated as having been obtained in violation of this chapter, and an inventory shall be served as provided for in subsection (d) of this section on the person named in the application.

(8)(a) The contents of any wire, oral, or electronic communication intercepted by any means authorized by this chapter shall, if possible, be recorded on tape or wire or other comparable device. The recording of the contents of any wire, oral, or electronic communication under this subsection shall be done in such a way as will protect the recording from editing or other alterations. Immediately upon the expiration of the period of the order, or extensions thereof, such recordings shall be made available to the judge issuing such order and sealed under his directions. Custody of the recordings shall be wherever the judge orders. They shall not be destroyed except upon an order of the issuing or denying judge and in any event shall be kept for ten years. Duplicate recordings may be made for use or disclosure pursuant to the provisions of subsections (1) and (2) of section 2517 of this chapter for investigations. The presence of the seal provided for by this subsection, or a satisfactory explanation for the absence thereof, shall be a prerequisite for the use or disclosure of the contents of any wire, oral, or electronic communication or evidence derived therefrom under subsection (3) of section 2517.

(b) Applications made and orders granted under this chapter shall be sealed by the judge. Custody of the applications and orders shall be wherever the judge directs. Such applications and orders shall be disclosed only upon a showing of good cause before a judge of competent jurisdiction and shall not be destroyed except on

order of the issuing or denying judge, and in any event shall be kept for ten years.

(c) Any violation of the provisions of this subsection may be punished as contempt of the issuing or denying judge.

(d) Within a reasonable time but not later than ninety days after the filing of an application for an order of approval under section 2518(7)(b) which is denied or the termination of the period of an order or extensions thereof, the issuing or denying judge shall cause to be served, on the persons named in the order or the application, and such other parties to intercepted communications as the judge may determine in his discretion that is in the interest of justice, an inventory which shall include notice of—

- (1) the fact of the entry of the order or the application;
- (2) the date of the entry and the period of authorized, approved or disapproved interception, or the denial of the application; and
- (3) the fact that during the period wire, oral, or electronic communications were or were not intercepted.

The judge, upon the filing of a motion, may in his discretion make available to such person or his counsel for inspection such portions of the intercepted communications, applications and orders as the judge determines to be in the interest of justice. On an ex parte showing of good cause to a judge of competent jurisdiction the serving of the inventory required by this subsection may be postponed.

(9) The contents of any wire, oral, or electronic communication intercepted pursuant to this chapter or evidence derived therefrom shall not be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in a Federal or State court unless each party, not less than ten days before the trial, hearing, or proceeding, has been furnished with a copy of the court order, and accompanying application, under which the interception was authorized or approved. This ten-day period may be waived by the judge if he finds that it was not possible to furnish the party with the above information ten days before the trial, hearing, or proceeding and that the party will not be prejudiced by the delay in receiving such information.

(10)(a) Any aggrieved person in any trial, hearing, or proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the contents of any wire or oral communication intercepted pursuant to this chapter, or evidence derived therefrom, on the grounds that—

- (i) the communication was unlawfully intercepted;
- (ii) the order of authorization or approval under which it was intercepted is insufficient on its face; or
- (iii) the interception was not made in conformity with the order of authorization or approval.

Such motion shall be made before the trial, hearing, or proceeding unless there was no opportunity to make such motion or the person was not aware of the grounds of the motion. If the motion is granted, the contents of the intercepted wire or oral communication, or evidence

derived therefrom, shall be treated as having been obtained in violation of this chapter. The judge, upon the filing of such motion by the aggrieved person, may in his discretion make available to the aggrieved person or his counsel for inspection such portions of the intercepted communication or evidence derived therefrom as the judge determines to be in the interests of justice.

(b) In addition to any other right to appeal, the United States shall have the right to appeal from an order granting a motion to suppress made under paragraph (a) of this subsection, or the denial of an application for an order of approval, if the United States attorney shall certify to the judge or other official granting such motion or denying such application that the appeal is not taken for purposes of delay. Such appeal shall be taken within thirty days after the date the order was entered and shall be diligently prosecuted.

(c) The remedies and sanctions described in this chapter with respect to the interception of electronic communications are the only judicial remedies and sanctions for nonconstitutional violations of this chapter involving such communications.

(11) The requirements of subsections (1)(b)(ii) and (3)(d) of this section relating to the specification of the facilities from which, or the place where, the communication is to be intercepted do not apply if—

(a) in the case of an application with respect to the interception of an oral communication—

(i) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant

Attorney General, or an acting Assistant Attorney General;

(ii) the application contains a full and complete statement as to why such specification is not practical and identifies the person committing the offense and whose communications are to be intercepted; and

(iii) the judge finds that such specification is not practical; and

(b) in the case of an application with respect to a wire or electronic communication—

(i) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General;

(ii) the application identifies the person believed to be committing the offense and whose communications are to be intercepted and the applicant makes a showing that there is probable cause to believe that the person's actions could have the effect of thwarting interception from a specified facility;

(iii) the judge finds that such showing has been adequately made; and

(iv) the order authorizing or approving the interception is limited to interception only for such time as it is reasonable to presume that the person identified in the application is or was reasonably

proximate to the instrument through which such communication will be or was transmitted.

(12) An interception of a communication under an order with respect to which the requirements of subsections (1)(b)(ii) and (3)(d) of this section do not apply by reason of subsection (11)(a) shall not begin until the place where the communication is to be intercepted is ascertained by the person implementing the interception order. A provider of wire or electronic communications service that has received an order as provided for in subsection (11)(b) may move the court to modify or quash the order on the ground that its assistance with respect to the interception cannot be performed in a timely or reasonable fashion. The court, upon notice to the government, shall decide such a motion expeditiously.