No.

IN THE
Supreme Court of the United States

MICHAEL CAREY,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

On Petition For A Writ Of Certiorari To The United States Court Of Appeals For The Ninth Circuit

PETITION FOR A WRIT OF CERTIORARI

ROBERT A. BATISTA
JOSHUA R. ZUCKERMAN
GIBSON, DUNN & CRUTCHER LLP
1050 Connecticut Avenue, N.W.
Washington, DC 20036

ALLYSON N. HO
Counsel of Record
BRADLEY G. HUBBARD
STEPHEN J. HAMMER
GIBSON, DUNN & CRUTCHER LLP
2001 Ross Avenue, Suite 2100
Dallas, Texas 75201
(214) 698-3100
aho@gibsondunn.com

Counsel for Petitioner

QUESTION PRESENTED

Whether courts lack power to fashion judge-made exceptions to the exceptionless suppression provisions of the Wiretap Act.

PARTIES TO THE PROCEEDING AND RULE 29.6 STATEMENT

1. Petitioner Michael Carey was the defendant in the district court and the appellant in the court of appeals.

Respondent the United States of America was the plaintiff in the district court and the appellee in the court of appeals.

2. Petitioner is an individual.

STATEMENT OF RELATED PROCEEDINGS

Petitioner is aware of the following related cases:

- *United States* v. *Carey*, No. 18-50393 (9th Cir.) (judgment entered Mar. 9, 2023; re-hearing en banc denied May 18, 2023);
- *United States* v. *Carey*, No. 21-50122 (9th Cir.) (voluntarily dismissed Sept. 16, 2022);
- *United States* v. *Carey*, No. 20-50353 (9th Cir.) (dismissed for want of prosecution Mar. 26, 2021);
- *United States* v. *Carey*, No. 14-50222 (9th Cir.) (judgment entered Sept. 7, 2016);
- *United States* v. *Carey*, No. 3:11-cr-00671-WQH-1 (S.D. Cal.) (judgment entered Apr. 23, 2014; judgment re-entered Oct. 25, 2018).

Petitioner is unaware of any other directly related cases in this Court or any other court, within the meaning of Rule 14.1(b)(iii).

TABLE OF CONTENTS

TABLE OF APPENDICES

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Constitutional Provisions

Statutes

Rules

Other Authorities

PETITION FOR A WRIT OF CERTIORARI

Petitioner Michael Carey respectfully petitions for a writ of certiorari to review the judgment of the United States Court of Appeals for the Ninth Circuit.

OPINIONS BELOW

The first order of the district court denying Carey's suppression motion (Pet. App. 42a–52a) isn't reported but is available in the Westlaw database at 2012 WL 1900059 (S.D. Cal. May 24, 2012). The first opinion of the court of appeals (Pet. App. 20a–41a) is reported at 836 F.3d 1092 (9th Cir. 2016). The second order of the district court denying Carey's suppression motion (Pet. App. 7a–19a) is reported at 342 F. Supp. 3d 1003 (S.D. Cal. 2018). The second opinion of the court of appeals (Pet. App. 1a–6a) isn't reported but is available in the Westlaw database at 2023 WL 2423338 (9th Cir. Mar. 9, 2023).

JURISDICTION

The court of appeals entered judgment on March 9, 2023. Pet. App. 1a–6a. The court of appeals denied Carey's petition for rehearing en banc on May 18, 2023. Pet. App. 62a. On July 25, 2023, Justice Kagan extended the time within which to file this petition to September 15, 2023. Order, No. 23A62 (July 25, 2023). On August 21, 2023, Justice Kagan extended the time within which to file this petition to October 15, 2023. Order, No. 23A62 (Aug. 21, 2023). This Court's jurisdiction is invoked under 28 U.S.C. § 1254(1).

CONSTITUTIONAL AND STATUTORY PROVISIONS INVOLVED

Relevant constitutional and statutory provisions are reproduced in the Appendix. Pet. App. 63a–97a.

INTRODUCTION

The text of the Wiretap Act is clear and categorical: "no part" of any communication intercepted in violation of the Act and "no evidence derived therefrom may be received in evidence." 18 U.S.C. § 2515. The Ninth Circuit held that the wiretap order in this case "did not authorize agents to listen to Carey [the defendant] or his associates." Pet. App. 33a Under the statute's plain language, that should have spelled the end of the matter—no order authorizing agents to listen to Carey's calls, no admissible evidence derived from those calls.

Instead, the Ninth Circuit kept this case alive by rewriting the Wiretap Act's exceptionless suppression rule to include an exception for "evidence obtained in 'plain hearing'"—even if it was intercepted "without having complied with the Wiretap Act." Pet. App. 23a–24a.

That decision deepens an acknowledged conflict among federal courts of appeals and state high courts over whether the Wiretap Act's suppression provisions admit of judicially created exceptions. The Sixth and D.C. Circuits and the Oregon and Kansas Supreme Courts have recognized that the text of the statute leaves no room for courts to adopt free-floating exceptions. But the Fourth, Eighth, and Eleventh Circuits have held the opposite—imposing exceptions on exceptionless provisions based on their reading of legislative history and their own policy judgments. By allowing the government to use wiretap evidence it

was "not authorize[d]" to intercept under the statute, Pet. App. 33a, the Ninth Circuit exacerbated this already entrenched conflict.

The Ninth Circuit's decision lacks any basis in the statute Congress adopted. While the Wiretap Act contains an abundance of exceptions, carveouts, and provisos, its suppression provisions contain none. They create a simple—and mandatory—rule: suppression is required if communications are "unlawfully intercepted" or if "the interception was not made in conformity with the [wiretap] order." 18 U.S.C. §§ 2515, 2518(10)(a)(i), (iii). If Congress had intended to create exceptions to those rules, it would have done so expressly. But it chose not to—and courts must respect that determination.

The lingering uncertainty over the scope of the Wiretap Act's suppression provisions carries important consequences. Congress's overarching concern in adopting the express limitations in the Wiretap Act was protecting Americans' privacy from increasingly powerful and invasive surveillance techniques. Judge-made exceptions to the Wiretap Act's suppression provisions—the cornerstone of that protective regime—threaten Congress's objective and leave criminal defendants to the vagaries of judicial policymaking.

This Court should resolve this conflict and enforce the Wiretap Act's suppression provisions as written.

STATEMENT

1. Title III of the Omnibus Crime Control and Safe Streets Act of 1968, also known as the Wiretap Act, 18 U.S.C. §§ 2510–2523, is "a comprehensive scheme for the regulation of wiretapping and electronic surveillance." *Gelbard* v. *United States*, 408

U.S. 41, 46 (1972). The Wiretap Act was enacted "[l]argely in response" to this Court's decisions in *Berger* v. *New York*, 388 U.S. 41 (1967), and *Katz* v. *United States*, 389 U.S. 347 (1967), which taken together held that electronic surveillance was subject to the restrictions of the Fourth Amendment. *Bartnicki* v. *Vopper*, 532 U.S. 514, 522–23 (2001).

"Much of" the Wiretap Act "was drawn to meet the constitutional requirements for electronic surveillance enunciated by this Court" in *Berger* and *Katz*. *United States* v. *U.S. Dist. Ct. for E. Dist. of Mich.*, 407 U.S. 297, 302 (1972). For example, to resolve constitutional defects identified in those cases, the Act requires courts to make particularized findings of probable cause before authorizing wiretaps. 18 U.S.C. § 2518(3)(a)–(b), (d); see *Berger*, 388 U.S. at 55–56, 58–59; *Katz*, 389 U.S. at 358.

But the Act also goes beyond the constitutional baseline in important respects. See *Visa Mktg., LLC* v. *Burkett*, 812 F.3d 954, 969 (11th Cir. 2016); *United States* v. *Nelson-Rodriguez*, 319 F.3d 12, 32 (1st Cir. 2003). For example, in addition to making particularized probable cause findings, the authorizing court must find that a wiretap is necessary because "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)(c).

One crucial respect in which the Act departs from the Fourth Amendment is with regard to remedies. The Fourth Amendment "is silent about how [it] is to be enforced." *Davis* v. *United States*, 564 U.S. 229, 231 (2011). "To supplement the bare text" of the Fourth Amendment, "this Court created the exclusionary rule," which is itself subject to judicially cre-

ated exceptions. *Id.* at 231–32, 237–38. But the Wiretap Act is entirely different. Unlike the Fourth Amendment, the Wiretap Act expressly mandates suppression—with no exceptions—if communications are "unlawfully intercepted" or if "the interception was not made in conformity with the [wiretap] order." 18 U.S.C. §§ 2515, 2518(10)(a)(i), (iii).

The result of Congress's efforts is a statute with formidable privacy safeguards. While the Wiretap Act "set out to provide law enforcement officials with some of the tools thought necessary to combat crime," *Scott* v. *United States*, 436 U.S. 128, 130 (1978), "the protection of privacy was an overriding congressional concern," *Gelbard*, 408 U.S. at 48. Congress's focus on privacy is reflected in three key features of the Act.

First, to prevent law enforcement from "unnecessarily infringing upon the right of individual privacy," *Scott*, 436 U.S. at 130, the Act "*flatly prohibit[s]*" "all interceptions of wire and oral communications" "[e]xcept" those interceptions that the Act itself "expressly authorize[s]," *Gelbard*, 408 U.S. at 46 (emphasis added); see also *United States* v. *Giordano*, 416 U.S. 505, 514 (1974).

Second, "to make doubly sure that the statutory authority [conferred on law enforcement] be used with restraint and only where the circumstances warrant," and to ensure that this authority is "not * * * routinely employed as the initial step in criminal investigation," "Congress legislated in considerable detail in providing for applications and orders authorizing wiretapping." *Giordano*, 416 U.S. at 515.

Third, these carefully delineated "limitations" on authorizing wiretaps are to be "enforce[d]" via the Act's mandatory-suppression provision. *Gelbard*, 408

U.S. at 48–49 (citing 18 U.S.C. § 2515). This point was "articulate[d] clearly" in the Act's "congressional findings." *Ibid.* Congress found that privacy interests made it "necessary * * * to prohibit any unauthorized interception of [wire or oral] communications, *and the use of the contents thereof in evidence* in courts and administrative proceedings." Pub. L. No. 90-351, § 801(b), 82 Stat. 197, 211 (1968) (emphasis added).

2. Approval of a wiretap order "may not be given except upon compliance with stringent conditions." *Gelbard*, 408 U.S. at 46; accord *Giordano*, 416 U.S. at 515 (Act "imposes important preconditions to obtaining any intercept authority at all"). To obtain a wiretap order, a federal agent must submit a detailed application to the court. The application must provide, among other information, "a full and complete statement of the facts and circumstances" that justify the officer's "belief that an order should be issued," including "details as to the particular offense that has been, is being, or is about to be committed," and "the identity of the person, if known, committing the offense and whose communications are to be intercepted." 18 U.S.C. § 2518(1)(b).

Upon receipt of an application, a court "may enter an ex parte order * * * authorizing or approving interception of wire, oral, or electronic communications," 18 U.S.C. § 2518(3), but only if the government has demonstrated:

(1) "probable cause" that "an individual is committing, has committed, or is about to commit a particular" enumerated offense;

(2) "probable cause" that the interception will obtain "particular communications concerning that offense";

(3) "probable cause" that the device or place proposed to be wiretapped is "being used, or [is] about to be used, in connection with the commission of such offense" by the target of the wiretap; and

(4) 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."

Ibid.

If the government satisfies these requirements and the court orders a wiretap, the order must "specify," among other things, "the identity of the person, if known, whose communications are to be intercepted." 18 U.S.C. § 2518(4)(a). And the wiretap order cannot last any "longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days." *Id.* § 2518(5).

Though Congress has strictly limited the use of wiretaps, it has also provided express exceptions from these requirements for exigent circumstances. For example, when an "emergency situation" involving "immediate danger of death or serious physical injury" requires a wiretap before an order can be obtained and there are grounds for approving the wiretap, the Act allows designated officials to conduct a wiretap so long as they apply for approval within 48 hours. 18 U.S.C. § 2518(7).

"[T]o enforce" the strict requirements of the Act, Congress authorized several remedies, including mandatory suppression of evidence obtained in violation of these requirements. *Gelbard*, 408 U.S. at 48–50; see also 18 U.S.C. § 2511(4) (criminal penalties);

id. § 2520 (civil action and relief); *id.* § 2521 (injunction). Specifically, if the government "unlawfully intercept[s]" communications or the interception is "not made in conformity with" the wiretap order, 18 U.S.C. § 2518(10)(a)(i), (iii), "no part of the contents" of those communications—"and no evidence derived therefrom"—"may be received in evidence in any trial, hearing, or other proceeding in or before any court," *id.* § 2515; see *Giordano*, 416 U.S. at 524 ("What disclosures are forbidden [by § 2515] is * * * governed by [§] 2518(10)(a) . . . ."). This "unequivocal" mandatory-suppression rule is a "plain command." *Gelbard*, 408 U.S. at 47, 51.

3. In 2010, federal agents secured a wiretap order for a phone number they believed to be associated with a conspiracy trafficking drugs from Mexico to the United States—the "Escamilla conspiracy." Pet. App. 23a–24a. As it turned out, the wiretap intercepted only conversations between petitioner Carey and his associates—none of whom had any connection to the targeted Escamilla conspiracy. Pet. App. 29a–30a. Through the wiretap, the agents obtained information that led to Carey's indictment for conspiracy to distribute cocaine. Pet. App. 25a.

Carey moved to suppress the evidence because the government hadn't complied with the Wiretap Act as to him and his associates. Pet. App. 25a; see 18 U.S.C. §§ 2515, 2518(10)(a). After the district court denied his suppression motion, Pet. App. 48a, Carey entered a conditional guilty plea, preserving his right to appeal the denial of that motion, Pet. App. 26a.[1]

---

[1] The basis for the district court's jurisdiction was 18 U.S.C. § 3231.

On appeal (*Carey I*), Carey argued that the government's failure to comply with the Wiretap Act required suppression. The Ninth Circuit agreed that the wiretap order failed to satisfy "the Wiretap Act requirements of probable cause and necessity" as to the alleged Carey conspiracy and therefore "did not authorize agents to listen to Carey or his associates." Pet. App. 23a–24a, 33a. Yet the Ninth Circuit nevertheless held that suppression wasn't required as long as the evidence was obtained "in 'plain hearing'"—that is, as long as it was obtained before agents "knew or should have known" that the intercepted conversations were unrelated to the targeted conspiracy. Pet. App. 23a–24a.

The *Carey I* panel made no attempt to ground its plain-hearing exception in any provision of the Wiretap Act. Instead, it fashioned the exception "by analogy" to the Fourth Amendment's plain-view doctrine. Pet. App. 30a. The panel remanded for the district court to apply this newly created exception in the first instance. Pet. App. 34a–35a.

On remand, the district court again denied Carey's suppression motion, concluding that all of the wiretap evidence was obtained before agents knew or should have known that they were listening to an unrelated conspiracy. Pet. App. 16a–19a. On appeal (*Carey II*), the Ninth Circuit found no error in the district court's application of the plain-hearing exception and affirmed. Pet. App. 2a–3a. Carey petitioned for rehearing en banc, which the Ninth Circuit denied. Pet. App. 62a.

REASONS FOR GRANTING THE PETITION

The Ninth Circuit's decision recognizing a plain-hearing exception to the Wiretap Act's suppression

provisions deepens an entrenched conflict among federal circuit courts and state high courts over whether the Act admits of judicially created exceptions. While four courts have enforced the Act's plain text, four others (now including the Ninth) have departed from the plain text based on their reading of legislative history and their own policy judgments.

That departure from plain text is unjustified. "The statute means what it says," *Dahda* v. *United States*, 138 S. Ct. 1491, 1498 (2018), and the job of courts is to enforce—not alter—the statutory text. Although Congress chose to include express exceptions in other portions of the Wiretap Act, it didn't include any in the Act's suppression provisions. The Ninth Circuit attempted to justify its departure from the Act's language by analogizing the Act to the Fourth Amendment, but the analogy doesn't work because the Amendment lacks the express suppression requirements that Congress enacted here.

This issue is exceptionally important because Congress carefully designed the Wiretap Act to protect Americans from the abuse of powerful surveillance tools. By allowing courts to poke holes in the Act's express suppression provisions based on their own policy views, the Ninth Circuit's decision jeopardizes the entire protective scheme. This Court's intervention is needed to ensure that the Act is enforced as written.

This case provides an ideal vehicle for doing so. The Ninth Circuit's creation of a plain-hearing exception was outcome determinative. The court expressly held that the wiretap order "did not authorize agents to listen to Carey or his associates," Pet. App. 33a, yet it allowed the government to avoid suppression based

on the plain-hearing exception alone. Deciding the viability of that exception will resolve the conflict and ensure the uniform application of the Act throughout the nation.

I. THE NINTH CIRCUIT'S DECISION DEEPENS AN ENTRENCHED CONFLICT AMONG FEDERAL AND STATE COURTS.

Federal and state courts are sharply divided over the propriety of judicially created exceptions to the Wiretap Act's suppression provisions. While several courts have recognized that the Wiretap Act's categorical text leaves no room for such exceptions, other courts have created exceptions based on legislative history or policy concerns.

A. Two circuit courts and two state high courts have rejected judicially created exceptions to the Wiretap Act's suppression provisions.

The Sixth Circuit has held that the good-faith exception to the Fourth Amendment's exclusionary rule recognized in *United States* v. *Leon*, 468 U.S. 897 (1984), can't be read into the Wiretap Act's suppression provisions. *United States* v. *Rice*, 478 F.3d 704, 711 (6th Cir. 2007). The Sixth Circuit focused on the Act's plain language, observing that in contrast to the Fourth Amendment, "the law governing electronic surveillance via wiretap is codified in a comprehensive statutory scheme providing explicit requirements, procedures, and protections." *Id.* at 712. Because "[t]he statute is clear on its face and does not provide for any exception," the Sixth Circuit held that "[c]ourts must suppress illegally obtained wire communications." *Ibid.*

The Sixth Circuit rejected the argument that the Wiretap Act allowed for judicially created exceptions.

While the "judicial branch created the exclusionary rule, and thus, modification of that rule falls to the province of the judiciary," in the Wiretap Act, "Congress has already balanced the social costs and benefits and has provided that suppression is the sole remedy for violations of the statute." *Rice*, 478 F.3d at 713. So the Sixth Circuit concluded that "[t]he rationale behind judicial modification of the exclusionary rule is * * * absent with respect to warrants obtained under [the Wiretap Act's] statutory scheme." *Ibid.*[2] The Sixth Circuit acknowledged that its decision conflicts with those of the Fourth, Eighth, and Eleventh Circuits. *Id.* at 713–14.

The D.C. Circuit has followed suit in declining to "import a good faith exception to [the Wiretap Act's] remedy of suppression." *United States* v. *Glover*, 736 F.3d 509, 515–16 (D.C. Cir. 2013), *abrogated on other grounds by Dahda*, 138 S. Ct. 1491. In the Wiretap Act, the D.C. Circuit observed, "Congress has spoken"—and put judicial exceptions off limits. *Id.* at 516.

The Oregon Supreme Court has also held that the Wiretap Act's suppression provisions don't admit of exceptions—rejecting, in that case, a good-faith exception. *State* v. *Harris*, 509 P.3d 83, 93 (Or. 2022), *cert. denied*, 143 S. Ct. 485 (2022). Like the Sixth Circuit, the Oregon Supreme Court reasoned from the text: "There is no basis for applying" a good-faith exception

---

[2] *Rice* distinguished *United States* v. *Baranek*, 903 F.2d 1068 (6th Cir. 1990), which held that suppression wasn't required for a conversation overheard while a wiretapped phone was off the hook, as a "narrow holding confined to its facts." 478 F.3d at 713. *Baranek* is inapposite to this case because there, unlike here, the wiretap order authorized the monitoring of the individuals who were overheard. 903 F.2d at 1069.

"in the context of a statute that specifically provides for the suppression and exclusion of evidence intercepted through an unlawful wiretap." *Ibid.*

The Kansas Supreme Court has reached the same conclusion. *State* v. *Bruce*, 287 P.3d 919, 926 (Kan. 2012). Acknowledging the "federal circuit split" on the issue, the court observed that *Leon* "sets forth a court-created exception to what was already a court-created remedy," while the Wiretap Act violation before it "was statutory; and both the federal and state statutory schemes include their own, explicit remedies of evidence exclusion." *Id.* at 925–26. So the court concluded there was no reason to sidestep the "statutorily provided remedy of suppression." *Id.* at 926.

B. By contrast, four circuit courts—including the Ninth Circuit below—have held that the Wiretap Act's suppression provisions contain unwritten exceptions.

The Eighth Circuit has read a good-faith exception into the Wiretap Act's suppression provisions. *United States* v. *Moore*, 41 F.3d 370, 376 (8th Cir. 1994), *cert. denied*, 514 U.S. 1121 (1995). It acknowledged that "*Leon* of course dealt with the judicially developed exclusionary rule for Fourth Amendment violations, whereas" the Wiretap Act included "a statutory exclusionary rule imposed for a 'violation of this chapter.'" *Ibid.*

But the Eighth Circuit nonetheless concluded that importing a good-faith exception into the Act was justified because the Act is supposedly "worded to make the suppression decision discretionary ('If the motion is granted')" and because the Act's "legislative history expresses a clear intent to adopt suppression principles developed in Fourth Amendment cases." *Moore*,

41 F.3d at 376 (citing S. Rep. No. 90-1097 (1968), *as reprinted in* 1968 U.S.C.C.A.N. 2112, 2185). One member of the panel, however, declined to join the portion of the court's opinion importing a good-faith exception into the statute. *Id.* at 377 (Bright, J., concurring).

The Fourth Circuit has taken the same tack. *United States* v. *Brunson*, 968 F.3d 325, 334 (4th Cir. 2020). It, too, recognized that *Leon* involved an exception to "the *judicially created* exclusionary rule" as opposed to the Wiretap Act's "*statutory* exclusionary rule." *Ibid.* But—based on the same legislative history and *Leon*'s "rationale"—it also held that it could read a good-faith exception into the Act. *Ibid.* A dissenting member of the panel observed, however, that "the statute does not provide a good faith exception" and faulted the majority for "disregard[ing]" "policy judgments already expressly made by Congress." *Id.* at 342 (Motz, J., dissenting).

The Eleventh Circuit has likewise imported a good-faith exception into the statute's suppression provisions. *United States* v. *Malekzadeh*, 855 F.2d 1492, 1497 (11th Cir. 1988), *cert. denied*, 489 U.S. 1029 (1989). The court took for granted that a good-faith exception could be read into the Act because suppression "would afford none of the deterrence served by the exclusionary rule." *Ibid.*

C. The Ninth Circuit's decision below further entrenched this conflict by joining the three circuits that have fashioned atextual exceptions to the Wiretap Act's suppression provisions.

At the outset, the Ninth Circuit held in no uncertain terms that the wiretap order "*did not authorize* agents to listen to Carey or his associates" because

"the wiretap order does not extend to unknown people not involved in the Escamilla conspiracy." Pet. App. 32a–33a (emphasis added). Yet the Ninth Circuit nevertheless concluded that—so long as the officers did not "know or reasonably should [have] know[n]" about the violation—"[t]he government may use evidence" obtained from the wiretap, and suppression isn't required. Pet. App. 24a, 33a. That is a good-faith exception in all but name. See *United States* v. *Franz*, 772 F.3d 134, 147 (3d Cir. 2014) (good-faith exception to Fourth Amendment exclusionary rule depends on what officers who obtained and executed warrant "knew or should have known").

Labels aside, the Ninth Circuit aligned itself with the Fourth, Eighth, and Eleventh Circuits—and against the Sixth and D.C. Circuits and Oregon and Kansas Supreme Courts—in concluding that the Wiretap Act's explicit suppression requirement can be disregarded based on officers' "objective reasonableness." *Leon*, 468 U.S. at 924. The conflict over whether the Wiretap Act's suppression provisions admit of judicially created exceptions is deeply entrenched and squarely presented here.

II. THE NINTH CIRCUIT'S DECISION IS WRONG.

The Wiretap Act's plain language requires suppression when the government unlawfully intercepts communications or the interception isn't made in conformity with the wiretap order. The *Carey I* panel held that the government erred in just these respects. Suppression should have followed as night follows day. Yet rather than apply the Act as written, the Ninth Circuit created a plain-hearing exception out of whole cloth. That exception has no basis in the Act's text, which provides no warrant for judicial policy-making.

A. The Wiretap Act's Mandatory-Suppression Rule Admits Of No Exceptions.

The Wiretap Act provides that if the government "unlawfully intercept[s]" communications or the interception is "not made in conformity with" the wiretap order, those communications—and all evidence derived from them—must be suppressed. 18 U.S.C. §§ 2515, 2518(10)(a)(i), (iii). That rule applies straightforwardly here. Because the *Carey I* panel held that the wiretap order "did not authorize agents to listen to Carey or his associates," Pet. App. 33a, the wiretap evidence should have been suppressed.

"[T]he starting point, as in all statutory construction, is the precise wording chosen by Congress in enacting [the Wiretap Act]." *United States* v. *Kahn*, 415 U.S. 143, 151 (1974). Because the Act's text is "clear," the Ninth Circuit's inquiry should have "beg[u]n and end[ed]" there. *Star Athletica, LLC* v. *Varsity Brands, Inc.*, 580 U.S. 405, 414 (2017). Under the Wiretap Act, if one of the grounds for suppression in Section 2518(10)(a) is met, the wiretapped communications (and all evidence derived from those communications) *must* be suppressed, as this Court has held, and as the Ninth Circuit itself recognized in this case. See *Giordano*, 416 U.S. at 524–28 (evidence obtained from an "unlawfully intercepted" communication under Section 2518(10)(a)(i) "*must* be suppressed under 18 U.S.C. § 2515") (emphasis added); Pet. App. 27a (evidence obtained "in violation of the statute * * * is inadmissible").[3]

---

[3] This Court has interpreted Section 2518(10)(a)(i) to apply to constitutional violations and statutory violations that implicate

The Wiretap Act's suppression rules contain no exceptions. And the remainder of the Act shows that Congress knows how to create exceptions when it wants to. In addition to requiring suppression, Congress authorized an action for civil damages against persons or entities (other than the United States) that intercept communications in violation of the Act, and expressly carved out exceptions to *that* remedy. See 18 U.S.C. § 2520(a) (civil action); *id.* § 2511(2)(a)(ii) (exception for providers of wire or electronic communications services). Other exceptions, carveouts, and provisos abound throughout the Act. See, *e.g.*, *id.* §§ 2510, 2511, 2512, 2513, 2518(1)(b), (3)(d), (7)–(9), 2521 (numerous "except," "notwithstanding," and "unless" clauses); *United States* v. *Moore*, 452 F.3d 382, 386 & nn.5–6 (5th Cir. 2006) (per curiam) (discussing the express "law enforcement" and "consent" exceptions in Sections 2510(5)(a) and 2511(2)); *United States* v. *Van Poyck*, 77 F.3d 285, 291–92 (9th Cir. 1996) (same).

Because "Congress provide[d] exceptions" in other parts of the Act, "[t]he proper inference" is that Congress "limited the statute to the [exceptions] set forth." *United States* v. *Johnson*, 529 U.S. 53, 58 (2000). The inclusion of "express exception[s]" in a statute, this Court has explained, "implies that there are no other[s]." *Jennings* v. *Rodriguez*, 138

Congress's "core concerns." *Dahda*, 138 S. Ct. at 1497 (citing *Giordano*, 416 U.S. at 527). The existence of probable cause is indisputably one of those core concerns. See *Giordano*, 416 U.S. at 527. And while this Court has read Section 2518(10)(a)(ii) not to require suppression for surplus defects in wiretap orders, it did so based on its interpretation of the suppression provision itself—not by creating any exception. *Dahda*, 138 S. Ct. at 1498–1500.

S. Ct. 830, 844 (2018) (emphasis omitted); see also Antonin Scalia & Bryan A. Garner, *Reading Law: The Interpretation of Legal Texts* 107–11 (2012) (negative-implication canon). But the Act's suppression provisions contain no carveouts. Courts "must give effect to, not nullify, Congress's choice to include limiting language" in some parts of the Act "but not" in the suppression provisions. *Gallardo ex rel. Vassallo* v. *Marstiller*, 142 S. Ct. 1751, 1759 (2022).

Even beyond the unambiguous text, "[t]he larger structure and history" of the Act confirm what the text makes clear. *Comcast Corp.* v. *Nat'l Ass'n of Afr. Am.-Owned Media*, 140 S. Ct. 1009, 1015 (2020). Congress adopted the Act "to prohibit, on the pain of criminal and civil penalties, *all* interceptions of oral and wire communications, except those *specifically provided for* in the Act." *Giordano*, 416 U.S. at 514 (emphases added; footnote omitted). So Congress's intention for courts to suppress wiretap evidence intercepted in violation of the Act is as clear as the language it enacted to accomplish that purpose.

Congress established a simple rule: If one of the conditions in Section 2518(10)(a) applies, the evidence must be suppressed—full stop. Applying that rule in this case should have been straightforward. The government's wiretap of Carey and his associates "was not made in conformity" with the wiretap order and their communications were "unlawfully intercepted," so the wiretap evidence should have been suppressed. 18 U.S.C. §§ 2515, 2518(10)(a)(i), (iii).

B. The Ninth Circuit Exceeded Its Authority By Creating An Exception To The Wiretap Act's Mandatory-Suppression Rule.

Despite the Wiretap Act's clear text, the *Carey I* panel rewrote the statute to include an exception for all information obtained before agents "knew or should have known" that they were intercepting conversations unrelated to the targeted conspiracy. Pet. App. 23a–24a. This rewrite exceeded the proper judicial role. The panel's only justification for that overreach—a strained analogy to the Fourth Amendment's plain-view exception—provides little support for the Ninth Circuit's holding given the manifest textual differences between the Fourth Amendment and the Wiretap Act.

1. The judiciary's "proper role" in our constitutional scheme is "to apply, not amend, the work of the People's representatives." *Henson* v. *Santander Consumer USA Inc.*, 582 U.S. 79, 90 (2017). As "interpreters of the law," federal courts must interpret statutes as written and "avoid judicial legislation"—that is, "tamper[ing] with the text of [a] statute." The Federalist No. 78, at 526 (Alexander Hamilton) (Jacob E. Cooke ed., 1961) (first quote); *United States* v. *Nat'l Treasury Emps. Union*, 513 U.S. 454, 478–79 (1995) (second and third quotes). Even when a court believes it could "improve upon" Congress's work, it still must "apply the text" that Congress enacted. *EPA* v. *EME Homer City Generation, L.P.*, 572 U.S. 489, 508–09 (2014). Similarly, a court has "no roving license * * * to disregard clear language simply on the view that * * * Congress 'must have intended' something" different. *Michigan* v. *Bay Mills Indian Cmty.*, 572 U.S. 782, 794 (2014).

Fashioning a homespun exception to a statute—as the Ninth Circuit did here—is a paradigmatic example of impermissible judicial policymaking. Courts have no authority to "elaborate unprovided-for exceptions to a text." Scalia & Garner, *supra*, at 93. Rather, "[w]hen the words of a statute are unambiguous * * * [the] judicial inquiry is complete." *Barnhart* v. *Sigmon Coal Co.*, 534 U.S. 438, 462 (2002) (internal quotation marks omitted).

Recognizing that "Congress legislated in considerable detail" in the Wiretap Act, this Court has repeatedly admonished lower courts to hew to the Act's text, including its suppression provisions. *Giordano*, 416 U.S. at 515; see, *e.g.*, *Dahda*, 138 S. Ct. at 1498; *Kahn*, 415 U.S. at 151 (focus on "precise wording" of Act is important given potential "tension between th[e] two stated congressional objectives" of fighting crime and "protecting individual privacy"); *Gelbard*, 408 U.S. at 47, 51 (emphasizing "unequivocal language of" and "plain command" of Act's mandatory-suppression rule). The Ninth Circuit's departure from the Act's text flouts this Court's instruction.

2. In search of justification for its legislative rewrite, the panel asserted that it was adopting a principle "similar" to the Fourth Amendment's plain-view exception. Pet. App. 23a, 30a (citing dicta in *United States* v. *Ramirez*, 112 F.3d 849 (7th Cir. 1997)). But that analogy doesn't work because of the clear textual differences between the Fourth Amendment and the Wiretap Act that reflect Congress's policy in the Act of "strictly * * * limit[ing] the employment of [wiretapping] techniques of acquiring information." *Gelbard*, 408 U.S. at 47.

Because the Fourth Amendment prohibits only "*unreasonable* searches and seizures," U.S. Const.

amend. IV (emphasis added), "the ultimate touchstone of the Fourth Amendment is 'reasonableness,'" *Brigham City* v. *Stuart*, 547 U.S. 398, 403 (2006). As a result, while "searches and seizures inside a home without a warrant are presumptively unreasonable," *ibid.*, "the warrant requirement is subject to certain reasonable exceptions," *Kentucky* v. *King*, 563 U.S. 452, 459 (2011). Among those is the plain-view exception. See, *e.g.*, *Coolidge* v. *New Hampshire*, 403 U.S. 443, 464–65 (1971) (plurality opinion).

In contrast to the Fourth Amendment, no part of the Wiretap Act invokes a "reasonableness" standard. Congress knows how to draft statutes with capacious guidance of that sort—the Sherman Act, for example, "invokes the common law." *Bus. Elecs. Corp.* v. *Sharp Elecs. Corp.*, 485 U.S. 717, 732 (1988) (discussing 15 U.S.C. § 1). That isn't what Congress did here with the Wiretap Act. *If* one of the conditions in Section 2518(10)(a) is satisfied, *then* the evidence must be suppressed under Section 2515. The Wiretap Act leaves no room for maneuvering based on courts' own evaluations of "reasonableness."

The panel's reliance on the Fourth Amendment is also irreconcilable with *Giordano*, where this Court explicitly distinguished the Fourth Amendment's "judicially fashioned exclusionary rule" from the Act's statutory—and mandatory—suppression rule. 416 U.S. at 524.

In *Giordano*, the government invoked the Fourth Amendment in arguing that wiretap evidence "should not have been suppressed" even though the wiretap application "did not comply with the statutory requirements," because, in the government's view, the "unlawfully intercepted" condition of Sec-

tion 2518(10)(a)(i) was "limited to constitutional violations." 416 U.S. at 524–27. Noting that "[t]he issue does not turn on the judicially fashioned exclusionary rule aimed at deterring violations of Fourth Amendment rights, but upon the provisions of [the Wiretap Act]," this Court held that "[t]he words 'unlawfully intercepted' are themselves not limited to constitutional violations," and rejected the government's proposed limitation. *Ibid.*

Far from legitimizing the Ninth Circuit's legislative rewrite, the Fourth Amendment analogy crystallizes the court's error. By not adhering to the cardinal rule that courts must "presume Congress says what it means and means what it says," the Ninth Circuit went astray. *Simmons* v. *Himmelreich*, 578 U.S. 621, 627 (2016).

III. THE QUESTION PRESENTED IS IMPORTANT.

It is exceptionally important for the Court to resolve this conflict, eliminate the uncertainty that now clouds Wiretap Act suppression proceedings, and avoid the harmful practical consequences of judge-made exceptions to the Act's suppression provisions.

A. The Ninth Circuit's rewrite of the Act undermines Congress's carefully calibrated statutory scheme. "[T]he protection of privacy was an overriding * * * concern" for Congress in enacting the Wiretap Act. *Gelbard*, 408 U.S. at 48. In Congress's view, "prohibit[ing]" the fruits of "any unauthorized interception[s]" from being used "in evidence in courts" was "necessary" "to protect effectively the privacy of wire and oral communications." Pub. L. No. 90-351, § 801(b), 82 Stat. at 211.

Even by 1968, the "tremendous scientific and technological developments that ha[d] taken place in

the last century" had resulted in "the widespread use and abuse of electronic surveillance techniques." *Bartnicki*, 532 U.S. at 542–43 (Rehnquist, C.J., dissenting) (quoting S. Rep. No. 90-1097, at 67). The "privacy of communication [wa]s seriously jeopardized by these techniques of surveillance." *Ibid.* (quoting S. Rep. No. 90-1097, at 67). Criminal and civil sanctions weren't enough to protect privacy—instead, Congress chose also to deny "[t]he perpetrator" of unauthorized wiretaps "the fruits of his unlawful actions in civil and criminal proceedings." *Gelbard*, 408 U.S. at 50 (quoting S. Rep. No. 90-1097, at 69).

Congress's concern about rooting out unnecessary and intrusive government wiretaps was well founded. Just the year before, a presidential commission had determined that "law enforcement officers [were] invading the privacy of many citizens without control from the courts." The President's Comm'n on Law Enf't and the Admin. of Just., *The Challenge of Crime in a Free Society* 203 (Feb. 1967), https://tinyurl.com/34dnjj2f. The potential for invasive government wiretaps has only grown since 1968—making it all the more important for courts to enforce the "limitations" that the Wiretap Act places "upon invasions of individual privacy." *Gelbard*, 408 U.S. at 49–50. The mandatory-suppression rule is "central to [that] legislative scheme." *Id.* at 50.

In 2021 alone—the most recent year with full data—courts issued about 5,000 wiretap orders, which have led to over 11,000 arrests and 1,300 convictions as of December 31, 2022. U.S. Courts, *Wiretap Report 2022*, tbls. 7, 9 (Dec. 31, 2022), https://tinyurl.com/3x7ka4as. Given these numbers, it's vital that this Court resolve whether courts have power to create their own exceptions to the Act's suppression

provisions. The existing uncertainty surrounding this foundational criminal procedure statute is untenable.

The entrenched conflict over the creation of exceptions to the Act's suppression provisions is particularly intolerable given the need for uniformity in this area of the law. Congress intended the Act to "define on a *uniform* basis the circumstances and conditions under which the interception of wire and oral communications may be authorized" as well as "the use of the contents thereof in evidence in courts and administrative proceedings." *Gelbard,* 408 U.S. at 49 (emphasis added) (quoting Pub. L. No. 90-351, § 801(b), 82 Stat. at 211). The diametrically opposed approaches to the Act's suppression provisions that exist in the lower courts are inconsistent with that goal.

B. Any judicially created exception to a federal statute is worthy of this Court's attention, but that is especially so with exceptions to the Act's mandatory-suppression rule. Though the rule of lenity doesn't directly apply here because the Act is not itself a "penal law[]," *United States* v. *Wiltberger*, 18 U.S. (5 Wheat.) 76, 95 (1820), the principles animating the rule condemn the plain-hearing exception and other judge-made exceptions to the Act's mandatory-suppression rule. The rule of lenity provides that "ambiguity concerning the ambit of criminal statutes should be resolved in favor of" the defendant. *Rewis* v. *United States*, 401 U.S. 808, 812 (1971). So when "there are two rational readings of a criminal statute, one harsher than the other," courts should interpret the statute in favor of the criminal defendant unless Congress has clearly spoken otherwise. *McNally* v. *United States*, 483 U.S. 350, 359–60 (1987).

The rule of lenity, then, prohibits "punish[ment] for violating just-so rules concocted after the fact, or

rules with no more claim to democratic provenance than a judge's surmise about legislative intentions." *Wooden* v. *United States*, 142 S. Ct. 1063, 1083 (2022) (Gorsuch, J., concurring in the judgment). Newly minted judge-made exceptions to the Act's "unequivocal" suppression rule, *Gelbard*, 408 U.S. at 47, raise similar concerns.

IV. This Case Is An Excellent Vehicle To Resolve The Conflict.

This case provides the Court an ideal vehicle for answering the question presented and resolving the conflict regarding judge-made exceptions to the Wiretap Act's suppression provisions.

The question presented is properly preserved for review by this Court. As the *Carey I* panel made clear, Carey argued both before the district court and the Ninth Circuit that the wiretap evidence should be suppressed because the wiretap order didn't authorize the agents to listen to Carey or his associates. Pet. App. 27a–28a. And the *Carey I* panel squarely rejected that argument, holding that even though the wiretap order "did not authorize agents to listen to Carey or his associates," any evidence obtained in "plain hearing" need not be suppressed. Pet. App. 33a.

That this issue was resolved on Carey's first appeal is no impediment to this Court's review. It's well settled that the Court has "authority to consider questions determined in earlier stages of the litigation where certiorari is sought from the most recent of the judgments of the Court of Appeals." *MLB Players Ass'n* v. *Garvey*, 532 U.S. 504, 508 n.1 (2001) (per curiam); see also *Mercer* v. *Theriot*, 377 U.S. 152, 153–54 (1964) ("We now consider all of the substantial federal questions determined in the earlier stages of the

litigation * * * for it is settled that we may consider questions raised on the first appeal . . . .") (internal quotation marks omitted).

And there's no doubt that the question presented is outcome dispositive. The *Carey I* panel held that "the government [could] *only* use evidence obtained in accordance with the 'plain hearing' doctrine." Pet. App. 33a (emphasis added). Neither the *Carey I* panel nor the *Carey II* panel identified any possible alternative basis for admission of the "critical wiretap evidence." Pet. App. 2a.

So the suppression issue turns entirely on whether there is a plain-hearing exception to the Wiretap Act's suppression provisions. No plain-hearing exception, no admissible evidence. And if none of the evidence is admissible, the Ninth Circuit must reverse the district court's suppression ruling, vacate the judgment of conviction, and remand so that Carey may withdraw his guilty plea, which was conditioned on his right to appeal the district court's suppression ruling. Pet. App. 2a, 26a; see Fed. R. Crim. P. 11(a)(2).

Carey unquestionably retains a concrete stake in the outcome of his appeal. He is currently on supervised release because of his challenged conviction, Pet. App. 53a–61a, and the restrictions imposed by the terms of his supervised release constitute a concrete injury. See *Spencer* v. *Kemna*, 523 U.S. 1, 7 (1998). And even after his supervised release ends, he will continue to suffer collateral consequences of his conviction that preclude mootness. See *Sibron* v. *New York*, 392 U.S. 40, 57–58 (1968).

CONCLUSION

The petition for a writ of certiorari should be granted.

Respectfully submitted.

ROBERT A. BATISTA
JOSHUA R. ZUCKERMAN
GIBSON, DUNN & CRUTCHER LLP
1050 Connecticut Avenue, N.W.
Washington, DC 20036

ALLYSON N. HO
Counsel of Record
BRADLEY G. HUBBARD
STEPHEN J. HAMMER
GIBSON, DUNN & CRUTCHER LLP
2001 Ross Avenue, Suite 2100
Dallas, Texas 75201
(214) 698-3100
aho@gibsondunn.com

Counsel for Petitioner

October 13, 2023

APPENDIX

TABLE OF CONTENTS

Page

APPENDIX A

NOT FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA, Plaintiff-Appellee, v. MICHAEL CAREY, AKA Garrocha, Defendant-Appellant.	No. 18-50393 D.C. No. 3: 11-cr-00671-WQH-1 MEMORANDUM*
	March 9, 2023

Appeal from the United States District Court
for the Southern District of California
William Q. Hayes, District Judge, Presiding.

Argued and submitted February 15, 2023
Pasadena, California

Before: WALLACE, HURWITZ, and BADE, Circuit Judges.

* This disposition is not appropriate for publication and is not precedent except as provided by Ninth Circuit Rule 36-3.

After Michael Carey was indicted for conspiracy to distribute cocaine, he moved to suppress evidence obtained by federal agents, claiming that the evidence was the fruit of a wiretap targeting a different drug-trafficking conspiracy (the "Escamilla conspiracy"). The district court denied the motion to suppress, and Carey pleaded guilty, reserving the right to challenge the district court's order on appeal. We vacated the suppression order and remanded for further proceedings because "[t]he record does not indicate what evidence was obtained before the agents knew or should have known they were listening to calls outside of the Escamilla conspiracy." *United States v. Carey*, 836 F.3d 1092, 1098 (9th Cir. 2016). On remand, the district court held an evidentiary hearing and found that the critical wiretap evidence was obtained before agents knew or should have known that they were listening to calls outside the targeted conspiracy, and the district court denied the motion to suppress. We have jurisdiction under 28 U.S.C. § 1291 over Carey's appeal from that ruling and affirm.

1. As a preliminary matter, we reject the government's argument that the plea agreement waived some of the issues Carey now raises on appeal. The agreement reserved Carey's right to "appeal the district court's ruling . . . denying his motion to suppress the wiretap." Each issue raised in this appeal attacks the denial of the suppression motion.

2. Regardless of the standard of review employed, the district court did not err in finding that there were "no interceptions on the T-14 line after any agent knew or should have known that the phone calls on the T-14 line could involve callers outside the scope of the Escamilla conspiracy." Finding the testimony of

the federal investigators "entirely consistent and credible," the court credited their statements that the relevant intercepted calls involved the same activity expected from members of the Escamilla conspiracy. The court also found credible the investigators' testimony that a five-day gap between initiation of the T-14 wiretap and the first intercepted conversation was not unusual and that not all Escamilla conspirators discarded their phones every twenty days. And although the first call intercepted under the wiretap order was in English—which Ignacio Escamilla had not previously used when talking to a government informant—the investigators declared that all other calls intercepted thereafter were in Spanish. Because the intercepted calls discussed a similar drug-trafficking operation, the investigators reasonably believed they "had found a previously undiscovered aspect of our subjects' drug trafficking activities," not an unrelated conspiracy.

Carey asserts that the federal investigators should have used border-crossing information to identify him and his co-conspirators, then discovered an ongoing Immigration and Customs Enforcement investigation into them, and then determined that the calls related to a distinct conspiracy. The seizure of the evidence occurred only one week after the first intercepted call, and the record does not show that the information Carey cites was readily accessible to the investigators or that protocol reasonably required them to query multiple databases during that brief period.

3. We also reject Carey's argument that he had a reasonable expectation of privacy in using T-14 during the relevant period. Under the "plain hearing" doctrine, the "government may use evidence obtained

from a valid wiretap prior to the officers' discovery of a factual mistake that causes or should cause them to realize that they are listening to phone calls erroneously included within the terms of the wiretap order." *Carey*, 836 F.3d at 1098 (cleaned up).

4. Carey argues for the first time on appeal that investigators' declarations and testimony were perjurious. But there "can virtually never be clear error," let alone plain error, if a district court credits the testimony of a witness who "has told a coherent and facially plausible story that is not contradicted by extrinsic evidence." *Earp v. Davis*, 881 F.3d 1135, 1145–46 (9th Cir. 2018) (cleaned up). Carey also asserts that the government improperly withheld "signal intelligence," but has not shown that any such information either exists or "would have changed the result of the proceeding." *United States v. Zuno-Arce*, 44 F.3d 1420, 1425 (9th Cir. 1995) (cleaned up).

5. Citing a statement in *United States v. Rodriguez* that a "different district court judge must decide any motion to suppress wiretap evidence, creating a second level of review in the district court," 851 F.3d 931, 937 (9th Cir. 2017), Carey argues for the first time on appeal that the judge who authorized the T-14 wiretap should not have considered the motion to suppress. But Carey's motion to suppress did not require the issuing judge to engage in a second level of review of his own wiretap authorization because Carey did not attack the validity of the wiretap in the district court following remand. Rather, the sole issue concerned information obtained after the issuance of the order.

6. Carey also challenges the district court's rejection of his request to replace retained counsel with appointed counsel. Reviewing for abuse of discretion, *see*

United States v. Rivera-Corona, 618 F.3d 976, 978 (9th Cir. 2010), we find none. The district court rejected Carey's informal pro per motion for substitution of counsel as improperly formatted but did not preclude the refiling of a properly formatted motion. Carey never refiled, and the district court did not abuse its discretion in failing to sua sponte grant the request, particularly given the need to control its docket in light of an imminent deadline for briefing on the motion to suppress. *See United States v. Gonzalez-Lopez*, 548 U.S. 140, 152 (2006) (stating that a district court has "wide latitude in balancing the right to counsel of choice against the needs of fairness and against the demands of its calendar" (cleaned up)).

7. Carey argues that the district court abused its discretion in denying discovery of various recorded calls, investigative material, and grand jury transcripts. Carey, however, has failed to show how the discovery was "material to preparing the defense." Fed. R. Crim. P. 16(a)(1)(E). The additional material would not have been relevant to the investigators' belief that they were intercepting Escamilla conspiracy calls before the seizure.

8. For the first time on appeal, Carey argues that the affidavit submitted in support of the wiretap application contained intentionally false or misleading statements and that intercepts were extraterritorial. Even assuming these arguments are not waived under Federal Rule of Criminal Procedure 12(c)(3) and are "thus reviewed for plain error," *United States v. Mongol Nation*, 56 F.4th 1244, 1252 (9th Cir. 2023), the arguments fail. Carey made no "substantial preliminary showing" of a "false statement" or that investigators acted "knowingly and intentionally, or with reckless disregard for the truth." *Franks v. Delaware*,

438 U.S. 154, 155-56 (1978). Nor has he demonstrated interception of relevant calls outside of the territorial jurisdiction of the district court, 18 U.S.C. § 2518(3), which includes both "where the tapped phone is located *and* where law enforcement officers first overhear the call," *United States v. Luong*, 471 F.3d 1107, 1109 (9th Cir. 2006).[1]

AFFIRMED.

---

[1] The government's motion to strike, **Dkt. 82**, is denied. Carey's motion to compel delivery of mail, **Dkt. 61**, is denied.

APPENDIX B

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA, Plaintiff, v. MICHAEL CAREY, Defendant.	CASE NO. 11CR671 WQH ORDER Oct. 25, 2018

HAYES, Judge:

The matter before the Court is the motion to suppress wiretap evidence (ECF No. 57) remanded to this Court on an open record by the Court of Appeals for the Ninth Circuit.

BACKGROUND

On October 4, 2016, the Court of Appeals for the Ninth Circuit vacated the order denying Defendant's motion to suppress evidence obtained from wiretaps and remanded "on an open record to determine what evidence was lawfully obtained in 'plain hearing.'" *United States v. Carey*, 836 F.3d 1092, 1094 (9th Cir. 2016). The Court of Appeals stated:

> [B]ecause the order did not authorize agents to listen to Carey or his associates, the government may only use evidence obtained in accordance with the "plain hearing" doctrine discussed above.
>
> The record does not indicate what evidence was obtained before the agents knew or

> should have known that they were listening to calls outside of the Escamilla conspiracy.

Id. at 1098. On remand, the parties agreed that the court would hold an evidentiary hearing to determine whether the FBI agents knew or reasonably should have known that the calls intercepted on T-14 during the period March 10, 2010 to March 17, 2010 were unrelated to the Escamilla conspiracy.

On April 16, 2018, after lengthy delay to accommodate Defendant's discovery request, the Court set an evidentiary hearing for May 30, 2018 with the agreement of both sides. (ECF No. 328).

On May 30, 2018 and July 6, 2018, the Court held the evidentiary hearing.

FACTS

FBI Special Agent Meltzer was assigned to the Cross Border Violence Task Force focused on drug-related violent crimes in 2009 and 2010. Agent Meltzer testified that he was the case agent for the investigation of a drug-trafficking group called the Heredia-Escamilla Organization, led by Armando Villareal-Heredia, who resided in Tijuana, Mexico. In February 2010, federal authorities obtained the first federal order to tap phones as part of the investigation. On March 5, 2010, federal authorities obtained a second order to tap phones for the investigation, including T-14 believed to be used by Escamilla Estrada. Meltzer was the affiant on the wiretap. Agent Meltzer stated in the affidavit in support of the wiretap application, and testified at the evidentiary hearing, that an informant had consensually recorded more than forty calls with Escamilla Estrada at the T-14 number from February 9, 2010 to March 4, 2010.

Agent Meltzer testified that the first intercepted call on T-14 occurred on March 10, 2010 in the English language with the speaker stating that this was "Mr. Keys' new number." Meltzer testified that the calls subsequently intercepted on T-14 were in the Spanish language. Agent Meltzer testified that he believed the calls intercepted on T-14 clearly concerned drug-trafficking. Meltzer testified that the investigators concluded at some point that Escamilla Estrada was not using T-14 and that they did not know the identity of the new user. Agent Meltzer testified that he thought the investigation had found a previously undiscovered aspect of the subject drug trafficking as often happens during wiretap investigations.

Agent Meltzer testified that the interceptees from T-14 were smuggling narcotics from Mexico to the United States and transporting currency to Mexico consistent with the activity under investigation in the Escamilla conspiracy. Agent Meltzer testified that it did not occur to him that the callers and calls on T-14 could be entirely unrelated to the target investigation because Escamilla Estrada had used T-14 as recently as the day before the court signed the second wiretap order. Agent Meltzer testified that he had information that the target conspiracy members were expected to change their phones every twenty-thirty days to avoid detection by law enforcement and that several phones in the target group, including the phone of Heredia, were used longer than thirty days.

Agent Meltzer testified that he was aware of cases where drug traffickers gave phones, sometimes temporarily, to associates in their criminal activity. Agent Meltzer testified that he had never heard of or contemplated a situation where a drug trafficker ac-

quired and used a phone just discarded by a completely unaffiliated drug trafficker, during a period of time when law enforcement was authorized to intercept calls on that phone. Agent Meltzer testified that he spoke with the prosecutor assigned to the investigation after concluding that Escamilla Estrada was not using T-14, and after intercepting calls indicating that T-14 was still being used to facilitate drug trafficking. Agent Meltzer testified that he recalled the prosecutor indicating that interceptions on T-14 could continue.

Agent Adkins of the Drug Enforcement Agency (DEA) testified that he was part of the Cross Border Violence Task Force during the Escamilla investigation. Agent Adkins testified that a surveillance log dated March 15, 2010 showed that five law enforcement representatives were a part of a surveillance team that followed a car and driver from the San Diego area up to Irvine and back to a residence in Chula Vista. Agent Meltzer testified that calls intercepted on T-14 on March 15, 2010 suggested that an unknown male would enter the United States, possibly with a drug load. Agent Meltzer testified that the calls on T-14 led to the surveillance by Agent Adkins and the surveillance team. Agents later identified the driver as Adrian Madrid, a codefendant later prosecuted with Defendant Carey.

Agent Meltzer testified that calls intercepted on T-14 led to a stop of a vehicle and the seizure of $688,000 in U.S. currency as well as a search warrant for a residence in Irvine where 17 kilograms of cocaine were found on March 17, 2010. Agent Meltzer testified that the user of T-14 stopped using the phone on that same day. Agent Meltzer testified that he

learned later that persons intercepted on T-14 and detained during the stop and search might be linked to an investigation conducted by agents for Homeland Security Investigations (HSI). Agent Meltzer testified that he met with HSI Agent Krall the day after the March 17 seizure. Agent Meltzer testified that he did not know Agent Krall prior to the meeting and that he had not been aware of the HSI investigation. Agent Meltzer testified that no overlap was discovered between his investigation and the Homeland Security investigation, other than the calls on T-14 and the March 17, 2010 stop and search.

Defendant Carey testified at the evidentiary hearing that he went to a cell phone storefront vendor located in Tijuana, Mexico on March 10, 2010 to purchase multiple new prepaid cell phones that would operate in both the United States and Mexico. Carey testified, "One of the phones I purchased had the number (619) 740-9230, which unbeknownst to me had been designated T-14 by the government in the wiretap order obtained on or about March 5, 2010 as part of the government's investigation of Ignacio Escamilla Estrada . . . , an investigation that had nothing to do with me or the associates later indicted with me." (ECF No. 337 at 2). "At 2:02 pm I used T-14 to call another phone to make sure they were in good working order. This test call is documented in a transcript of the call produced to me by the government as part of discovery." *Id*. Carey testified that he was not advised by the vendor that the number assigned to T-14 had been recycled in the previous days from a different handset. Carey testified that he left the phone in the possession of codefendant Jose Hernandez in Tijuana, Mexico on March 10, 2010 and returned to the United States.

HSI Agent Krall was affiliated with the Border Enforcement Security Task Force in approximately April of 2009 and began investigating a drug trafficking case that involved Defendant Carey and others. Agent Krall testified that he was aware of Carey and codefendants Adrian Madrid and Javier Lacarra. Agent Krall testified that he was not aware of Jose Hernandez. Agent Krall testified that "the MO of the organization was to cross the border with a spare tire loaded with . . . cocaine." (ECF No. 347 at 22). Agent Krall testified that he drew links to Carey from the arrest of Francisco Noriega in Mexico. Agent Krall wrote in a report that the investigation targeted "international drug smuggling cells with ties to firearms and bulk cash smuggling." *Id*. at 25. Agent Krall testified that his task force investigation included primarily HSI and DEA, and that ATF played a minor role. Agent Krall testified that he wrote reports and placed information into his agency database during the investigation sharing information with the investigating team.

Agent Krall testified that he installed a tracking device on Defendant Carey's vehicle early in 2010 and that the tracking device showed that Carey traveled to Irvine on February 21, 2010 and February 22, 2010.

Agent Krall testified that he learned of the March 17, 2010 seizure of drugs and money in the evening after the seizure. Agent Krall testified that he met with Agent Meltzer a day or two after the seizure. Agent Krall testified that prior to March 17, 2010, he did not know about the Irvine residence where the drugs were seized, he had not shared any information with Agent Meltzer, and he had not involved the FBI in his investigation at all.

CONTENTIONS OF THE PARTIES

Defendant Carey contends that Agent Meltzer knew or should have known well before the wiretap on T-14 went live on March 5, 2010 that there would be non-Escamilla target group speakers. Defendant asserts that any attempt at minimization would have quickly led the agents to conclude that the intercepted calls on T-14 were not pertinent to the Escamilla warrant. Defendant asserts that "the Escamilla co-conspirators communicated exclusively in Spanish and the Carey co-conspirators did not." (ECF No. 351 at 10). Defendant asserts that Agent Meltzer's familiarity with the violent drug trafficking methods of the Escamilla group should have led the agent to the conclusion that the calls intercepted on T-14 were unrelated to the Escamilla conspiracy. Defendant asserts that substantial overlap with the investigation of HSI Agent Krall establishes that Agent Meltzer realized at least as early as March 15, 2010 that the target of his wiretap was not Escamilla but rather Carey and his coconspirators. Defendant asserts that Agent Meltzer knew that the Escamilla targets utilized a "use and drop" policy regarding cell phones. Defendant asserts that there was no reason for him to believe that there would be a wiretap on a new phone that he purchased in a sealed box.

Plaintiff United States contends that agents were unable to conclusively determine whether Carey or others intercepted on T-14 from March 10, 2010 to March 17, 2010 were involved in the activities targeted by the Cross Border Task Force. Plaintiff United States asserts that Agent Melzer and Agent Krall did not find any overlap between their investigations beyond the T-14 intercepts and the March 17

seizures but never concluded that the persons intercepted on T-14 were not a part of the Escamilla organization. Plaintiff United States asserts that the agents had no reason to question whether the drug dealings on T-14 were connected to the Escamilla target prior to the March 17 seizures and the stop of the intercepts on T-14. Plaintiff United States asserts that the agents had no reason to suspect or conclude that an unrelated drug trafficker had acquired and used a discarded tapped phone. Plaintiff United States asserts that Agent Meltzer reasonably concluded that Escamilla Estrada had given the phone to an unidentified associate in the Escamilla conspiracy.

APPLICABLE LAW

> The Fourth Amendment provides an exception to the warrant or probable cause requirement when police see contraband in "plain view." We adopt a similar principle today and hold that the police may use evidence obtained in "plain hearing" when they overhear speakers unrelated to the target conspiracy while listening to a valid wiretap, without having complied with the Wiretap Act requirements of probable cause and necessity as to those specific speakers. However, the agents must discontinue monitoring the wiretap once they know or reasonably should know that the phone calls only involved speakers outside the target conspiracy. *Cf. Maryland v. Garrison*, 480 U.S. 79, 87, 107 S.Ct. 1013, 94 L.Ed.2d 72 (1987).

Carey, 836 F.3d at 1093–94. In *Maryland v. Garrison*, the police officers obtained a search warrant for McWebb's apartment. 480 U.S. at 80. At the time the

officers obtained the search warrant, the officers "reasonably believed that there was only one apartment on the premises described in the warrant. In fact, the third floor was divided into two apartments, one occupied by McWebb and one by respondent Garrison." *Id*. After entering Garrison's apartment and finding heroin, cash, and drug paraphernalia, the officers realized that the third floor contained two apartments and discontinued the search. At the time of the search, "[a]ll of the officers reasonably believed that they were searching McWebb's apartment." *Id*. at 81. In deciding whether to suppress the evidence the officers found in Garrison's apartment, the Supreme Court stated that "we must judge the constitutionality of their conduct in light of the information available to them at the time they acted." *Id*. at 85. The Supreme Court concluded:

> If the officers had known or should have known, that the third floor contained two apartments before they entered the living quarters on the third floor, and thus had been aware of the error in the warrant, they would have been obligated to limit their search to McWebb's apartment. Moreover, as the officers recognized, they were required to discontinue the search of respondent's apartment as soon as they discovered that there were two separate units on the third floor and therefore were put on notice of the risk that they might be in a unit erroneously included within the terms of the warrant. The officers' conduct and the limits of the search were based on the information available as the search proceeded. . . .

> [T]he validity of the search of respondent's apartment pursuant to a warrant authorizing the search of the entire third floor depends on whether the officers' failure to realize the overbreadth of the warrant was objectively understandable and reasonable. Here it unquestionably was. The objective facts available to the officers at the time suggested no distinction between McWebb's apartment and the third-floor premises.

Id. at 86–88.

RULING OF THE COURT

In this case, the Court must determine whether the "agents knew or should have known that they were listening to calls outside of the Escamilla conspiracy." *Carey*, 836 F.3d at 1098. This determination must be made "in light of the information available to them at the time they acted." *Maryland v. Garrison*, 480 U.S. at 85.

Agent Meltzer obtained authorization to intercept the calls on T-14 by an order issued on March 5, 2010. Agent Meltzer reasonably believed that calls on T-14 were associated with the Heredia-Escamilla target investigation based upon information that an informant had consensually recorded more than forty calls in the Spanish language with Escamilla Estrada at the T-14 number from February 9, 2010 to March 4, 2010. There were no calls on T-14 for five days. On March 10, 2010, the initial call was in the English language with the speaker stating that this was "Mr. Keys' new number." The calls subsequently intercepted on T-14 from March 10, 2010 to March 17, 2010 were in the Spanish language. The calls between March 10, 2010 and March 17, 2010 were related to the smuggling of

narcotics from Mexico and the transportation of currency to Mexico, consistent with the target investigation.

Prior to March 17, 2010, Agent Meltzer was informed that the person using T-14 was not Ignacio Escamilla Estrada and that the calls remained consistent with the criminal activity under investigation. Agent Meltzer continued to reasonably believe that the person using T-14 was affiliated with the known targets or a person who was part of the Escamilla conspiracy. In light of the information available to Agent Meltzer prior to March 17, 2010, Agent Meltzer reasonably believed that the T-14 calls were related to the Escamilla investigation. Agent Meltzer did not know and had no reason to know that the person using T-14 from March 10, 2010 to March 17, 2010 could be unrelated to the Escamilla conspiracy. Agent Meltzer had no way to know that a phone with the T-14 number was for sale at a cell phone storefront vendor located in Tijuana on March 10, 2010. Agent Meltzer had no way to know that a purportedly unrelated drug dealer had purchased a phone with the T-14 number and used the phone to sell controlled substances in a conspiracy unrelated to the Escamilla conspiracy.

On March 17, 2010, Agent Meltzer learned that the information intercepted from the T-14 line led to the drug seizure at the Irvine residence, and that the associated individuals could be linked to a separate investigation conducted by HSI Agent Krall. This link was confirmed two days later when Agent Meltzer met with DEA and HSI agents, and it was determined that there was no additional overlap between the two investigations. No communications were intercepted on T-14 after the agent determined that the two investigations were separate. There were no interceptions

on the T-14 line after any agent knew or should have known that the phone calls on the T-14 line could involve callers outside the scope of the Escamilla conspiracy and the scope of the wiretap order.

The testimony provided by Agent Meltzer and Agent Krall was entirely consistent and credible. The agents worked separate investigations. There is no evidence that Agent Meltzer or Agent Krall were aware of any overlap between their investigations or should have been aware of any overlap. The March 15, 2010 surveillance did not provide any facts to indicate that T-14 was not being used by the Escamilla organization. The "objective facts available to [the agents prior to March 17, 2018] suggested" that T-14 continued to be used by the Escamilla conspirators. *See Maryland v. Garrison*, 480 U.S. at 88. The agents did not know and had no reason to know that the person speaking on the tapped line was not involved in the target conspiracy. The Court concludes that the agents were not required to cease the wiretap and the motion to suppress the evidence is denied.

In this case, Defendant entered a conditional guilty plea pursuant to Fed. R. Crim. P 11(a)(2) which states:

> With the consent of the court and the government, a defendant may enter a conditional plea of guilty or nolo contendere, reserving in writing the right to have an appellate court review an adverse determination of a specific pretrial motion. A defendant who prevails on appeal may then withdraw the plea.

Fed. R. Crim. P 11(a)(2). The "specific pretrial motion" reserved for appeal was Defendant's motion to

suppress wiretap evidence,[1] and Defendant's motion to wiretap suppress the wiretap evidence is denied. Having not succeeded in suppressing any evidence, there is no "erroneously denied suppression motion" which contributed to the Defendant's "decision to plead guilty." *See United States v. Lustig*, 830 F.3d 1075, 1087 (9th Cir. 2016). Defendant has not prevailed on appeal and is not entitled to withdraw his plea under Rule 11(a)(2). The Judgment entered on April 23, 2014 is reentered for the purposes of any further appeal.[2]

IT IS HEREBY ORDERED that the motions to suppress wiretap evidence (ECF Nos. 57, 351) are denied. The Judgment entered on April 23, 2014 is hereby reentered for the purposes of any further appeal. Any Notice of Appeal must be filed "within 14 days" of this order. Fed. R. App. P. 4 (b)(1).

DATED: October 25, 2018

/s/ William Q. Hayes
WILLIAM Q. HAYES
United States District Judge

---

[1] ECF No. 57.

[2] The minute entry (ECF No. 282) entered on October 4, 2016 is vacated.

APPENDIX C

FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA, *Plaintiff-Appellee*, v. MICHAEL CAREY, AKA Garrocha, *Defendant-Appellant*.	No. 14-50222 D.C. No. 3:11-cr-00671-WQH-1 OPINION

Appeal from the United States District Court
for the Southern District of California
William Q. Hayes, District Judge, Presiding

Argued and Submitted May 6, 2016
Pasadena, California

Filed September 7, 2016

Before: Alex Kozinski, William A. Fletcher, and Ronald M. Gould, Circuit Judges.

Opinion by Judge Gould;
Dissent by Judge Kozinski

SUMMARY*

Criminal Law

The panel vacated the district court's order denying the defendant's motion to suppress evidence derived from the use of wiretaps.

The panel held that police may use evidence obtained in "plain hearing" when they overhear speakers unrelated to the target conspiracy while listening to a valid wiretap, without having complied with the Wiretap Act requirements of probable cause and necessity as to those specific speakers, but that agents must discontinue monitoring the wiretap once they know or reasonably should know that the phone calls only involved speakers outside the target conspiracy.

Because the record does not show exactly when agents knew or should have known that the phone conversations did not involve the persons involved in the target conspiracy, the panel vacated the district court's denial of the motion to suppress and remanded to the district court on an open record to determine what evidence was lawfully obtained in "plain hearing."

Judge Kozinski dissented from the part of the opinion where the majority remands on an open record. He wrote that if the record does not show whether the agents reasonably believed that the conspiracies were related until after a traffic stop, the defendant, who presented no evidence contradicting an agent's sworn declaration, has only himself to blame.

---

* This summary constitutes no part of the opinion of the court. It has been prepared by court staff for the convenience of the reader.

COUNSEL

Knut Sveinbjorn Johnson (argued) and Emerson Wheat, San Diego, California, for Defendant-Appellant.

Peter Ko (argued), Assistant United States Attorney, Chief, Appellate Section, Criminal Division; Laura E. Duffy, United States Attorney; United States Attorney's Office, San Diego, California; for Plaintiff-Appellee.

OPINION

GOULD, Circuit Judge:

Acting pursuant to the Wiretap Act, 18 U.S.C. §§ 2510–22, federal agents secured a wiretap order for a San Diego phone number based on evidence that Ignacio Escamilla Estrada (Escamilla) was using the number in a drug smuggling and distribution conspiracy. Agents monitoring the wiretap overheard drug-related phone conversations. At some point during a seven-day period, the agents realized that Escamilla was not using the phone. Agents continued listening, however, believing at least initially that the people speaking on the phone might have been part of the Escamilla conspiracy. The seven days of wiretap monitoring culminated in a traffic stop, and agents then confirmed that the persons on the phone had no connection to Escamilla.

Appellant Michael Carey was eventually identified as a speaker in some of the phone calls, and he was then charged with conspiracy to distribute cocaine. Carey moved to suppress the evidence obtained from the wiretaps, arguing that the government violated the Wiretap Act by never applying for a wiretap as to him or his coconspirators. The district court denied the motion, ruling that the government could rely on the Escamilla order to listen to Carey's conversations.

The Fourth Amendment provides an exception to the warrant or probable cause requirement when police see contraband in "plain view." We adopt a similar principle today and hold that the police may use evidence obtained in "plain hearing" when they overhear speakers unrelated to the target conspiracy while listening to a valid wiretap, without having

complied with the Wiretap Act requirements of probable cause and necessity as to those specific speakers. However, the agents must discontinue monitoring the wiretap once they know or reasonably should know that the phone calls only involved speakers outside the target conspiracy. *Cf. Maryland v. Garrison*, 480 U.S. 79, 87 (1987).

The district court did not apply these principles, and the record in this case does not show exactly when agents knew or should have known that the phone conversations did not involve Escamilla and his coconspirators. We vacate the district court's denial of Carey's motion to suppress and remand to the district court on an open record to determine what evidence was lawfully obtained in "plain hearing."

I

On March 5, 2010, the district court granted FBI Special Agent Christopher Melzer's application for a wiretap order for several phone numbers thought to be associated with a drug conspiracy led by Ignacio Escamilla Estrada (Escamilla). The phone number designated "T-14" was believed to belong to Escamilla. The wiretap of T-14 went live on March 5, although no calls were intercepted until March 10.

Starting on the 10th, the agents overheard "drug-related" calls, but at some point the agents realized that the person using T-14 was not Escamilla. The agents did not know who the people speaking on T-14 were, although Melzer initially "thought the callers and calls might still be affiliated with [the] known targets or part of the criminal activity [he] was investigating." Melzer consulted with federal prosecutors, and agents continued to monitor the calls.

On the morning of March 17, 2010, agents intercepted a call indicating that someone would be traveling with "invoices" (believed to be code for drug money). The agents coordinated with local police officers to execute a traffic stop on a car involved in the phone calls. Officers identified the driver as Adrian Madrid and searched the vehicle, finding cash and a cellphone tied to the T-14 number. Officers then obtained a search warrant for a related residence and found cocaine. Now knowing Madrid's identity, Melzer learned that there was an ongoing DEA/ICE investigation into Madrid and his associates. Melzer met with ICE and DEA agents, and they concluded that there was no "overlap" between the Madrid and Escamilla conspiracies.

Agents later identified Carey as a member of Madrid's conspiracy.[1] Carey was indicted in February 2011 for conspiracy to distribute cocaine in violation of 21 U.S.C. §§ 841(a)(1) and 846. He filed a motion to suppress "any and all evidence derived from the use of wiretaps," arguing that the government failed to comply with the Wiretap Act, 18 U.S.C. §§ 2510–22, with respect to Carey and his coconspirators. In Carey's view, the government instead had unlawfully "relie[d] on the validity of the Escamilla order to justify the independent and unrelated use of wiretap surveillance against Mr. Carey." Carey also requested a *Franks*[2] hearing to "fill in the holes" of a declaration by Special Agent Melzer that had been submitted to the district

---

[1] Phone calls intercepted by the wiretap referred to "Garrocha," apparently Carey's nickname, but the record does not show when agents made that connection. The record also does not reveal how Carey's associate, Jose Antonio Hernandez-Gutierrez, ended up with Escamilla's phone number.

[2] *See Franks v. Delaware*, 438 U.S. 154 (1978).

court to explain the agents' and officers' actions in connection with the wiretap.

The district court denied the motion to suppress, reasoning that the government had complied with the statute to obtain the wiretap order against Escamilla and holding that "[t]here was no requirement for a separate showing of necessity once the agents concluded that T-14 was not primarily used by Escamilla. The agents reasonably believed that the callers and calls might be affiliated with Escamilla or other offenses." Carey pled guilty in an agreement that preserved his right to appeal the denial of his motion to suppress. Carey's appeal was timely and we have jurisdiction under 28 U.S.C. § 1291.

II

In 1967, the Supreme Court issued two opinions discussing the constitutionality of certain phone surveillance techniques. In *Berger v. New York*, 388 U.S. 41 (1967), the Court invalidated a New York wiretap statute as "too broad in its sweep resulting in a trespassory intrusion into a constitutionally protected area." *Id*. at 44. Then in *Katz v. United States*, 389 U.S. 347 (1967), the Court held that federal agents violated the Fourth Amendment by eavesdropping on and recording a telephone call without a warrant. *Id*. at 348, 357–59.

Congress took note of these foundational decisions when passing the Omnibus Crime Control and Safe Streets Act of 1968. *See United States v. U.S. Dist. Ct. for the E. Dist. of Mich*., 407 U.S. 297, 302 (1972). Title III, which is known colloquially as the Wiretap Act, prescribes certain procedures that the government must follow to secure judicial authorization for a wiretap. *See United States v. Giordano*, 416 U.S. 505, 507

(1974) (citing 18 U.S.C. §§ 2510–20). The government must demonstrate probable cause that a particular offense has been or will be committed, *see* 18 U.S.C. § 2518(1)(b); *United States v. Kahn*, 415 U.S. 143, 155 (1974), and the government must demonstrate "necessity" for the wiretap by showing that traditional investigative procedures did not succeed or would be too dangerous or unlikely to succeed if tried, *see* 18 U.S.C. § 2518(1)(c); *United States v. Blackmon*, 273 F.3d 1204, 1207 (9th Cir. 2001). The statute also requires the government to adopt minimization techniques to "reduce to a practical minimum the interception of conversations unrelated to the criminal activity under investigation." *United States v. McGuire*, 307 F.3d 1192, 1199 (9th Cir. 2002); *see* 18 U.S.C. § 2518(5).

If the government uses a wiretap in violation of the statute, evidence obtained from the wiretap is inadmissible against the conversation's participants in a criminal proceeding. *Giordano*, 416 U.S. at 507–08; *see* 18 U.S.C. § 2515. Carey argues that suppression is warranted here because the government did not comply with these statutory requirements as to him or his coconspirators—the government's wiretap application instead demonstrated probable cause and necessity only as to Escamilla's conspiracy.

As a preliminary matter, the government argues that the only Wiretap Act argument Carey has preserved is his necessity argument: whether the agents violated 18 U.S.C. § 2518(1)(c) by listening to Carey's phone calls without first trying "other investigative procedures" or explaining "why they reasonably appear to be unlikely to succeed if tried or to be too dangerous." At oral argument on appeal, the government further suggested that Carey's argument that the gov-

ernment could not rely on the Escamilla wiretap to listen to Carey's calls was an argument about the proper "execution of the order" rather than "the necessity showing."

In this context, however, we see no meaningful difference between the argument presented to the district court and that presented on appeal. While Carey's suppression brief primarily discussed necessity, he argued in substance that the government could not "rel[y] on the validity of the Escamilla order to justify the independent and unrelated use of wiretap surveillance against Mr. Carey." The government recognized that this was the premise of Carey's argument, responding with its view that "agents properly continued to intercept T-14 even after determining Escamilla was not the primary user." And this claim was further fleshed out before the district court when, in dialogue with the judge, Carey's lawyer argued that "[a]t the point in that time during that 15-day period they [the agents] realize this is a separate and distinct conspiracy group of people, they have to stop" and "make the required showing, obtain the authorization for the wiretap for that separate and distinct group of people." Even on appeal the government recognizes in its brief that "the circumstances under which interception occurred" were placed "squarely at issue" in Carey's suppression motion, which charged that "Melzer knew, at the time of interception, the T-14 calls were 'unrelated to the Escamilla investigation.'"

Carey's arguments to the district court adequately conveyed the thrust of his argument on appeal that the Escamilla wiretap order did not authorize the government to listen to Carey's phone calls. Carey's claim is preserved.

III

Turning to the question whether agents could lawfully use the Escamilla wiretap to listen to Carey's conversations, we note that there is a lack of Ninth Circuit precedent squarely on point. While the Wiretap Act allows officials to intercept and use calls "relating to offenses other than those specified in the order of authorization or approval," 18 U.S.C. § 2517(5), we have found no case in which this statutory provision was used to authorize officers to listen to people who were unaffiliated with the initial wiretap subjects.[3] Carey cites several cases for the proposition that the necessity showing in a wiretap application must be specifically tailored to the target subjects,[4] but none of these cases involves a situation in which a concededly valid wiretap order was used to obtain evidence of an unrelated person's crime.

Here the government showed necessity and probable cause for a wiretap of the target conspiracy. But what happens when a wiretap that is valid at its inception is later used to listen to someone who is not

---

[3] *See United States v. Reed*, 575 F.3d 900, 911 (9th Cir. 2009) (allowing government to introduce calls of Jackson intercepted on a wiretap for Reed when agents initially thought the phone was Reed's, Jackson was a "previously unknown associate of Reed," and "the record shows that TT10 was being used in the furtherance of Reed's PCP enterprise"); *United States v. Baker*, 589 F.2d 1008, 1011 (9th Cir. 1979) (per curiam) (allowing government to introduce calls of Baker intercepted on a wiretap for Judd when Baker was speaking to Judd). While the government relies on these cases, it concedes that they "are not perfect fits."

[4] *See, e.g.*, *United States v. Staffeldt*, 451 F.3d 578, 579 (9th Cir. 2006); *United States v. Gonzalez, Inc.*, 412 F.3d 1102, 1115 (9th Cir. 2005); *Blackmon*, 273 F.3d at 1208–09.

involved in the conspiracy under surveillance? It is that novel question to which we turn our attention.

The Seventh Circuit has addressed a similar situation in dicta. Writing for that court, then-Chief Judge Posner explained, "It is true that if government agents execute a valid wiretap order and in the course of executing it discover that it was procured by a mistake and at the same time overhear incriminating conversations, the record of the conversations is admissible in evidence. It is just the 'plain view' doctrine translated from the visual to the oral dimension." *United States v. Ramirez*, 112 F.3d 849, 851 (7th Cir. 1997) (internal citations omitted). "But," the court continued, "once the mistake is discovered, the government cannot use the authority of the warrant, or of the [wiretap] order, to conduct a search or interception that they know is unsupported by probable cause or is otherwise outside the scope of the statute or the Constitution." *Id*. at 852 (citing *Maryland v. Garrison*, 480 U.S. 79, 87 (1987)).[5] We conclude that the Seventh Circuit's observations are persuasive.

These conclusions are drawn by analogy to Fourth Amendment case law. In *Maryland v. Garrison*, 480 U.S. 79 (1987), officers secured a warrant for Lawrence McWebb's residence at "2036 Park Avenue third floor apartment." *Id*. at 80. When the officers entered, they "reasonably concluded" that the third floor was only one apartment unit, but they soon discovered that the floor was divided into two apartments—one McWebb's, the other Garrison's. *Id*. at 81. Before the

---

[5] This discussion in *Ramirez* was dicta because the court held that the wiretap was not being used illegally when agents mistakenly listened to phone calls in Minnesota rather than Wisconsin. *Id*. at 852–53.

officers realized that, they saw drug contraband in Garrison's apartment. *Id*. at 80. The Court held that the search "[p]rior to the officers' discovery of the factual mistake" did not violate the Fourth Amendment so long as the officers' failure to realize the mistake "was objectively understandable and reasonable." *Id*. at 88.

But at the same time, the Court emphasized that the officers "were required to discontinue the search of respondent's apartment as soon as they discovered that there were two separate units on the third floor and therefore were put on notice of the risk that they might be in a unit erroneously included within the terms of the warrant." *Id*. at 87. We have applied this rule from Garrison in similar situations. *See, e.g.*, *Mena v. City of Simi Valley*, 226 F.3d 1031, 1038–39 (9th Cir. 2000); *Liston v. County of Riverside*, 120 F.3d 965, 979 (9th Cir. 1997) ("Until the officers learned that they were in the wrong house, the officers could have reasonably believed . . . that the way they conducted the search was lawful. . . . But once they knew the house belonged to the Listons, their search was no longer justified.").

Despite the Seventh Circuit's decision in *Ramirez*, both the government and Carey resist the application of this doctrine to the wiretap context. Carey states that *Garrison* "has limited application to wiretaps" because of the procedural requirements of the Wiretap Act. This argument is unavailing because the government did comply with the statute to get a valid wiretap for Escamilla on T-14. The question here is whether the government could use that valid wiretap to listen to unrelated people's phone calls—a concern that mirrors the question in *Garrison* whether officers

could rely on a valid warrant for entry into an unrelated person's apartment.

The government, on the other hand, argues that the agents could continue monitoring the wiretap even after realizing that they were not listening to the target conspiracy. The government urges that the wiretap order in this case authorized interception of drug calls by "others yet unknown" over T-14. In the government's view, Carey is such an unknown person. Read in context, however, the wiretap order does not extend to unknown people not involved in the Escamilla conspiracy.

Having carefully reviewed the full record, including any portions filed under seal, we conclude that the provisions of the wiretap order persuasively indicate that the unknown people referred to in the wiretap order must be involved with the Escamilla conspiracy; the order does not authorize the wiretap of "others yet unknown" participating in a *conspiracy* "yet unknown." Moreover, the wiretap order could not authorize surveillance of an unknown conspiracy because the statute requires agents to demonstrate probable cause and necessity to procure a wiretap order. 18 U.S.C. § 2518(1)(b)–(c). Agent Melzer's affidavit contained probable cause that "others yet unknown" were participating in the Escamilla conspiracy, but it understandably contained no information about unknown people engaged in drug trafficking outside the Escamilla conspiracy.

The government also argues that agents could listen to Carey's conversations because the Wiretap Act permits the collection of evidence of other crimes under 18 U.S.C. § 2517(5). That provision authorizes the government to use "communications relating to of-

fenses other than those specified in the order of authorization or approval." But importantly—and fatally to the government's argument—the statute does so only when officers are "engaged in intercepting wire, oral, or electronic communications in the manner authorized herein." 18 U.S.C. § 2517(5). Because the order does not authorize agents to listen to conversations by individuals outside the Escamilla conspiracy for the reasons stated above, this provision does not help the government here.

In short, we see no reason to depart from principles requiring cessation of a wiretap once the government knows or reasonably should know that the person speaking on the tapped line is not involved in the target conspiracy. *See Ramirez*, 112 F.3d at 851–52. The government may use evidence obtained from a valid wiretap "[p]rior to the officers' discovery of [a] factual mistake" that causes or should cause them to realize that they are listening to phone calls "erroneously included within the terms of the" wiretap order. *Cf. Garrison*, 480 U.S. at 87–88. And once the officers know or should know they are listening to conversations outside the scope of the wiretap order, they must discontinue monitoring the wiretap until they secure a new wiretap order, if possible. *Cf. id*. at 87.

IV

Applying this rule to Carey's case, we first note that Carey does not challenge the validity of the wiretap order as to Escamilla, so the agents were justified in initially listening to the conversations on T-14. But because the order did not authorize agents to listen to Carey or his associates, the government may only use evidence obtained in accordance with the "plain hearing" doctrine discussed above.

The record does not indicate what evidence was obtained before the agents knew or should have known that they were listening to calls outside of the Escamilla conspiracy. Melzer's declaration stated, "Within that time frame [March 10–17], after an amount of time that I do not recall exactly, we concluded that the person using T-14 was not Ignacio Escamilla Estrada. We also did not know the identities of the persons calling T-14." While Melzer's declaration suggests that he "thought the callers and calls might still be affiliated with" the Escamilla conspiracy, the record does not show whether he continued or reasonably could have continued to hold that belief through March 17. In fact, at some point agents consulted with federal prosecutors about whether they could or should continue to intercept calls on the wiretap.

It is unclear how much of the government's wiretap evidence may fall outside of the "plain hearing" doctrine. Because the parties staked out polarized positions before the district court—the government arguing for all wiretap evidence, Carey for none of it—and because the district court adopted the government's position in denying the motion to suppress, the record lacks the findings necessary to determine what evidence was admissible against Carey.[6] We vacate

---

[6] Carey "alternatively" sought a *Franks* hearing to "fill in the holes" in Melzer's declaration. But this request does not fit into the *Franks v. Delaware*, 438 U.S. 154 (1978), framework because the Melzer declaration was not an affidavit supporting a wiretap application. *See id*. at 171–72 (explaining purpose of *Franks* hearing is to explore possible falsehoods in affidavit supporting request for search warrant); *United States v. Ippolito*, 774 F.2d 1482, 1484–85 (9th Cir. 1985) (applying *Franks* to wiretap applications).

the district court's order denying the motion to suppress and remand on an open record to determine what evidence is admissible against Carey under the legal framework set forth above.

The dissent argues that Carey forfeited this relief by "fail[ing] to demonstrate in the district court that any evidence should be suppressed under the rule he advocated." Dissent at 22. This conclusion appears to stem from the dissent's premise that "Carey can hardly be surprised by the 'plain hearing' rule we adopt today" because he advocated for a similar rule in the district court. Dissent at 18.

We disagree with this conclusion and its premise. Carey's primary argument in the district court was broader than the rule we adopt today. He did not concede that any evidence should be admitted under a plain hearing rule. Instead, Carey contended that "any and all evidence derived from the use of wiretaps" should be suppressed. Carey argued that the agents learned at some point that they were listening to an unrelated conspiracy, and therefore the wiretap order was invalid because it did not establish necessity as to him.

Also, while the dissent is correct that Carey did not present evidence "contradicting Agent Melzer's sworn declaration," dissent at 18, Carey argued to the district court that Melzer's declaration was lacking "specifically what level of knowledge [the agents] had between – when the wiretap started on March 10th through to March 17th." The dissent repeatedly emphasizes that Carey did not contest the accuracy of Agent Melzer's declaration. This is true, but beside the point. Carey's objection was not that the declaration was inaccurate; his objection was that it was *incomplete*. The district court recognized Carey's belief

that "there are things that are not in his declaration that you believe would be relevant facts," and the court was aware of Carey's alternate request to take evidence about Melzer's level of knowledge regarding the relationship between Escamilla and the phone calls. But because the district court then applied the wrong legal standard, the district court did not believe that any additional evidence was necessary.[7]

As stated above, Carey and the government took polarized positions before the district court, and the correct legal standard lay somewhere in between. In such circumstances, we conclude that the proper course is to allow the parties to present more evidence on remand to determine whether any evidence should be suppressed under the proper legal standard that we have now declared.

VACATED AND REMANDED.

---

[7] The dissent faults us for this "oblique suggestion," dissent at 21, but it is clear to us that Carey was seeking a *Franks* hearing to learn more about Melzer's knowledge of the speakers heard over the wiretap. As we acknowledged above, *see* note 6 *supra*, that is not a proper purpose of a *Franks* hearing. But counsel's mislabeling of his request does not change the fact that Carey's counsel put the district court on notice that counsel thought additional evidence could be necessary to resolve the suppression motion. And had the district court applied the correct legal standard, it would have recognized additional evidence was needed.

KOZINSKI, Circuit Judge, dissenting:

I join my colleagues insofar as they hold that the government may use evidence obtained from a valid wiretap until "officers know or should know they are listening to conversations outside the scope of the wiretap order." Op. at 14. But I dissent from Part IV of the opinion where the majority remands with instructions that the district court apply this rule to Carey's case on an open record. If, as the majority recognizes, the "record does not show" whether the federal agents reasonably believed that the conspiracies were related until after the traffic stop, op. at 15, Carey has only himself to blame. He presented no evidence contradicting Agent Melzer's sworn declaration.

Carey can hardly be surprised by the "plain hearing" rule we adopt today: As the majority acknowledges, "Carey argued that the agents learned at some point that they were listening to an unrelated conspiracy," op. at 16, but he failed to identify a specific point. Instead, Carey relied *only* on the fact that the officers listened for seven days to the conversations on the phone.

But the length of time the officers listened is hardly dispositive of whether they realized or should have realized they were listening to a different conspiracy than the one covered by the warrant. That depends on what the officers heard and when they heard it. While agents eventually realized that Escamilla wasn't using the phone, the wiretap order also permitted them to intercept conversations of Escamilla's unknown co-conspirators. The agents could have reasonably believed that Escamilla had passed the phone to a confederate. FBI Agent Melzer declared under oath that he "thought the callers and

calls might still be affiliated with [the] known targets or part of the criminal activity [he] was investigating." He claims he didn't definitively learn until after the traffic stop that the calls were unrelated to the Escamilla conspiracy. By expressly refusing to challenge the Melzer declaration, Carey conceded the point.

The majority is mistaken in saying that "Carey's primary argument in the district court was broader than the rule we adopt today." Op. at 16. Here's what Carey's lawyer argued in his motion in the district court:

> Mr. Carey concedes the FBI reasonably believed the intercepted calls from T-14 could be related to the Escamilla conspiracy, at the beginning of interception. At some point, however, during the daily interceptions, with the number of calls mounting with new interceptees, it became less reasonable for the FBI to continue to believe this new conspiracy was related to Escamilla. As the Court is well aware, the FBI's investigation into the Escamilla conspiracy was vast and extensive. At some point, between March 10 to March 17, 2010, the FBI had to have realized that th[e] T-14 interceptions were part of a separate conspiracy—separate from, and unrelated to, the Escamilla conspiracy for which the wiretap was authorized.
>
> When they knew, they should have stopped, worked with other law enforcement agencies investigating the Carey conspiracy and proceeded with a proper, traditional investigation. Instead, the FBI, knowing at some point that they were no longer investi-

> gating Escamilla and his co-conspirators, continued to monitor T-14 under the auspices and authority of the Escamilla wiretap.

And here's what Carey's lawyer said to the district court during oral argument:

> It is our position that at some point along that week as the calls were coming in, as the interceptees were being intercepted and they were not connected to the Escamilla extensive investigation, that the reasonableness of that agent to believe that was somehow related to Escamilla diminished. It diminished per call per day, all the way to the end of the week that where it is unreasonable then—where it started out being reasonable by the end of the week [sic].

Carey never identified a specific point when it became unreasonable for the agents to believe that they were still listening to the Escamilla conspiracy. Carey was given full discovery and thus had access to the recordings and transcripts of the intercepted phone conversations. If he believed that the agents should have known prior to the traffic stop that this was a different conspiracy, he could have pointed this out to the district court. Instead, he offered no evidence and explicitly declined to dispute the accuracy of Melzer's statement:

> The Court: From your standpoint it is fair to say that you don't dispute the accuracy that Mr. Melzer set forth in his declaration? Your argument is that, well, there are things that are not in his declaration that you believe

would be relevant facts, but that as far as a—there is no disagreement with his declaration.

[Carey's lawyer]: That is an accurate statement.

The Court: So in deciding the motion, there is no objection to the Court relying on facts set forth in this declaration as true and as part of the record.

[Carey's lawyer]: I think that is a fair statement.

The majority is also mistaken in its oblique suggestion that Carey was seeking to obtain additional evidence or requested an evidentiary hearing "to take evidence about Melzer's level of knowledge regarding the relationship between Escamilla and the phone calls." Op. at 17. Here's what actually happened in the district court:

[The Court]: Is there any evidentiary—any witnesses in your view that would be necessary for an evidentiary hearing? It seems like it is a legal matter to me.

[Carey's lawyer]: Except for the Franks hearing—outside of the Franks hearing, I don't see a need for an evidentiary hearing, other than perhaps Agent Crawl (phonetic) from the DEA was conducting the investigation while the FBI was conducting the wiretap. Outside of that I don't see any other relevant evidentiary purposes.

Carey thus expressly disowned the purposes the majority generously attributes to him. As for the *Franks* hearing, the majority recognizes that it's inapplicable to this situation. Op. at 15.

This isn't a case where we've announced an unforeseen rule, surprising a defendant who didn't have the opportunity to argue about its application in the district court. Carey's problem is that he failed to demonstrate in the district court that any evidence should be suppressed under the rule he advocated. I would affirm the district court's judgment rather than give Carey a mulligan.

APPENDIX D

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA, Plaintiff, vs. MICHAEL CAREY (1) and ADRIAN MADRID (3), Defendant.	CASE NO. 11CR671 WQH ORDER May 24, 2012

HAYES, Judge:

The following motions are pending before the Court: (1) the Motion to Suppress Wiretap Evidence and to Order the Government to Produce a Bill of Particulars filed by Defendant Michael Carey (ECF No. 57); (2) the Motion to Suppress Evidence filed by Defendant Adrian Madrid; (ECF No. 69) and (3) Amended Motion to Suppress filed by Defendant Adrian Madrid (ECF No. 78).

On February 23, 2011, the grand jury returned an indictment against Defendants Michael Carey, Jose Antonio Hernandez-Gutierrez, Adrian Madrid, Cuauthemoc Arturo Armendariz-Sandoval, and Javier Lacarra for conspiracy to distribute cocaine in violation of 21 U.S.C. §§ 841(a)(1) and 846. (ECF No. 1).

BACKGROUND FACTS

In March 2010, the United States applied for an order authorizing the interception of wire communications over several phones, including (619) 740-9230

(hereinafter T-14). At the time of the application, T-14 was thought to be used by Ignacio Escamilla Estrada, a target in a FBI investigation. On March 5, 2010, the court authorized interception of T-14. From March 10, 2010 to March 17, 2010, agents repeatedly intercepted "drug-related" calls over T-14. (ECF No. 61-1 at 2). At some time during this one week period of monitoring, the agents concluded that the person using T-14 was not Ignacio Escamilla Estrada. The agents continued to monitor T-14 because almost all calls over T-14 were drug-related calls consistent with the criminal investigation underway.

An intercepted call on the morning of March 17, 2010 indicated that Madrid would be "coming down" with "invoices" on that day. (ECF No. 76-1 at 33.) In response to the call, investigators took up surveillance and observed Defendant Madrid arrive at an Irvine residence in a Jeep Cherokee. Armendariz backed a Toyota out of the residence's garage, and Defendant Madrid drove the Jeep Cherokee into the garage in its place. Two hours later, Defendant Madrid drove the Jeep Cherokee out of the garage and onto southbound Interstate 5.

Investigators informed an Orange County Sheriff's Deputy that the Jeep Cherokee could be involved with narcotics activity and instructed the deputy to develop independent cause for a stop of the vehicle in order to protect the overall investigation. The Sheriff Deputy took up position on the freeway to intercept the Jeep Cherokee. When the Jeep went by, the Sheriff Deputy pulled into traffic and followed the Jeep Cherokee for one and one-half miles. The Sheriff Deputy observed a broken tail light and stopped the Jeep Cherokee for a violation of Vehicle Code 24525(a).

The Sheriff's Deputy asked Defendant Madrid to exit the vehicle, frisked, and handcuffed him. The Deputy obtained consent to search the vehicle and utilized a narcotics detector dog to assist in the search. The dog alerted along the driver door panel, the rear quarter panel, and the entire rear cargo area. No drugs were discovered. Deputies discovered a black nylon bag in the rear compartment area which contained two large currency bundles of U.S. currency vacuum-sealed in plastic. The total amount seized was approximately $700,000. Deputies found two cell phones in the vehicle, including the phone that Defendant Madrid had been intercepted on earlier in the day.

On the same date, March 17, 2010, deputies obtained a search warrant for the Irvine residence. Armendariz was inside. Deputies discovered 17 kilograms of cocaine in a bedroom safe. Armendariz consented to a search of the Toyota, which contained three manufactured compartments and a false wall.

On or about March 17, 2010, Special Agent Christopher Melzer, the FBI lead investigator, learned that T-14 and associated individuals could be linked to a separate investigation being conducted by ICE and DEA. On March 19, 2010, Agent Melzer met with ICE and DEA agents and determined that there was no overlap between the two investigations other than the T-14 calls.

On July 7, 2010, an indictment was filed as a result of the Escamilla investigation, charging 43 individuals with conspiracy to conduct enterprise affairs through a pattern of racketeering activity. (*United States v. Heredia,* 10CR3044-WQH). In May and June 2011, defendants in the Escamilla case filed Motions to Suppress Wiretap Evidence. On August 24, 2011,

the Court issued a written order in *United States v. Heredia* denying all the Motions to Suppress Wiretap Evidence. (ECF No. 808).

I. Motion to Suppress Wiretap Evidence (ECF No. 57)

a. Contentions of the Parties

Defendant Carey contends the Court should suppress all evidence obtained as a result of the wiretaps conducted on T-14 because the affidavits in support of the warrant application failed to demonstrate necessity. Defendant contends the order denying the motion to suppress wiretap evidence in the Escamilla case (10CR3044 ECF No. 808) does not apply to the Carey conspiracy. Defendant asserts the Government was required to make a separate showing of necessity for the new conspiracy once it concluded that T-14 was not used by Escamilla in order to continue intercepting calls on T-14. Defendant contends that there has been no showing that the government tried traditional investigative procedures, nor made a showing that such attempts were reasonably unlikely to succeed if tried prior to intercepting his calls.

The Government contends that the affidavit established necessity for the wiretaps in the Escamilla investigation. The Government contends that the agents properly continued to intercept T-14 even after determining Escamilla was not the primary user. The Government contends that the intercepts may be used for prosecution even if they relate to offenses other than those named in the original order. The Government contends that there is no "prerequisite to interception . . . that the affidavit establish necessity to wiretap unknown persons who proved to be actual interceptees." (ECF No. 61 at 7-8).

b. Legal Standard

Authorization for a wiretap is based on probable cause to believe that the telephone is being used to facilitate the commission of a crime, and the order need not name any particular person if such person is unknown. *See* 18 U.S.C. § 2518(1)(b)(iv); *United States v. Kahn*, 415 U.S. 143, 157 (1974) (wiretap is proper when there is "probable cause to believe that a particular telephone is being used to commit an offense but no particular person is identifiable"); *United States v. Reed*, 575 F.3d 900, 911 (9th Cir. 2009) (agents properly continued to intercept phone after discovering that Jackson, not Reed - the original suspected user - was the "primary user" of the phone); *see also United States v. Nunez*, 877 F.2d 1470, 1473 n. 1 (10th Cir. 1989) ("[T]he government ha[s] no duty to establish probable cause as to each interceptee. It is sufficient that there was probable cause to tap the phone.").

Identification of individuals whose communications will be intercepted is required "if known." 18 U.S.C. § 2518(4)(a). The Supreme Court has concluded that "Congress could not have intended that the authority to intercept must be limited to those conversations between a party named in the order and others, since at least in some cases, the order might not name any specific party at all." *Kahn*, 415 U.S. at 157; *see also United States v. Homick*, 964 F.2d 899, 904 (9th Cir. 1992) (citing *Kahn*, 415 U.S. at 156–57) ("[T]he government may seek a wiretap authorization in order to discover the identities of suspected co-conspirators, and a conversation involving a party not named in the authorization that reveals that party's involvement in the criminal activity under investigation is admissible.").

The necessity requirement is directed to the objective of the investigation as a whole, and not to any particular person. If the Government can demonstrate that ordinary investigative techniques would not disclose information covering the scope of the drug trafficking enterprise under investigation, then it has established necessity for the wiretap. *See United States v. McGuire*, 307 F.3d 1192, 1197–99 (9th Cir. 2002). "[T]he government ha[s] no duty to establish [necessity] as to each possible interceptee. It is sufficient that there was [necessity] to tap the phone." *Nunez*, 877 F.2d at 1473 n. 1 (citations omitted).

Congress addressed situations where law enforcement officers intercept communications relating to offenses not named in the original order. 18 U.S.C. 2517(5) provides, "[w]hen an investigative or law enforcement officer, while engaged in intercepting . . . electronic communications relating to offenses other than those specified in the order of authorization or approval, the contents thereof, and evidence derived therefrom, may be disclosed or used as provided in subsections (1) and (2) of this section." Subsections (1) and (2) permit law enforcement officers to disclose the communications to another investigative or law enforcement officer to the extent such use is appropriate to the proper performance of his official duties. *Id*.

c. Ruling of the Court

In this case, the Government complied with the original wiretap authorization requirements, including necessity and minimization. This Court issued an order in *United States v. Heredia*, Case No. 10CR3044 WQH denying the defendants' Motion to Suppress Wiretap Evidence for Failure to Comply with Necessity and Minimization Requirements. (ECF No. 808 at 30). The Court concluded that the "affidavits in

support of each application provided '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' in compliance with 18 U.S.C. § 2518(1)(c)." (ECF No. 808 at 28–29).

The agents concluded Escamilla was not the primary user after an unspecified time of monitoring T-14. (ECF No. 61 at 2). There was no requirement for a separate showing of necessity once the agents concluded that T-14 was not primarily used by Escamilla. The agents reasonably believed that the callers and calls might be affiliated with Escamilla or other offenses. On March 17, 2010, Special Agent Melzer subsequently learned of a link to a separate investigation. This link was confirmed two days later when he met with DEA and ICE agents, and it was determined that there was no overlap between the two investigations. No communications were intercepted after the agent determined that the two investigations were separate.[1]

The Motion to Suppress Wiretap Evidence filed by Defendant Michael Carey is denied.

II. Motion to Order the Government to Issue a Bill of Particulars (ECF No. 57)

The purpose of a bill of particulars is to protect a defendant against a second prosecution for an inadequately described offense, and enable him to prepare an intelligent defense. *Duncan v. United States*, 392 F.2d 539, 540 (9th Cir. 1968). "Generally an indictment is sufficient if it sets forth the elements of the

---

[1] Defendant has made no showing of any facts which would require a *Franks* hearing.

charged offense so as to ensure the right of the defendant not to be placed in double jeopardy and to be informed of the offense charged." *United States v. Woodruff*, 50 F.3d 673, 676 (9th Cir. 1995). Often, full discovery "obviates the need for a bill of particulars." *United States v. Long*, 706 F.2d 1044, 1054 (9th Cir. 1983). A defendant is not entitled to know all the evidence the government intends to produce, but only the theory of the government's case. *Yeargain v. United States*, 314 F.2d 881, 882 (9th Cir. 1963).

The granting or refusal to grant the bill of particulars is a matter within the sound discretion of the trial court. *Wong Tai v. United States*, 273 U.S. 77 (1927); *see United States v. Buckner*, 610 F.2d 570, 574 (9th Cir. 1979). The indictment in this case provides a plain, concise, and definite written statement of the essential facts constituting the crime with which he has been charged, and was adequate under Fed. R. Crim. P. 7. The Government has provided Carey with complete discovery including "over 1400 pages of reports and other documents generated or obtained through the investigation." (ECF No. 61 at 12).

The Motion to Order the Government to Produce a Bill of Particulars is denied.

III. Motion to Suppress Evidence (ECF No. 69 and ECF No. 78).

a. Contentions of the Parties

Defendant Madrid contends the stop of his vehicle violated his Fourth Amendment rights. Madrid contends that his tail light was not broken on the day he was stopped. Madrid contends that even if the traffic stop was initially lawful, it was unlawfully prolonged by the additional searches by officers and the narcotic detector dog. Madrid contends that the Government

bears the burden of proving that he voluntarily and intelligently gave consent to search his vehicle. *Id*. Madrid contends that any evidence obtained as a result of the Fourth Amendment violation must be suppressed including the subsequent seizure at the Irvine residence.

The Government contends that the collective knowledge of the investigators provided probable cause to stop and search the vehicle. The Government contends that repeated, intercepted calls of Defendant Madrid and others during the preceding seven days indicated Defendant Madrid was involved in receiving, off-loading, and transporting drug shipments in the United States and transporting currency to Mexico. The Government contends agents observed Madrid parking his vehicle in a closed garage, departing shortly thereafter and driving south towards Mexico. The Government contends the intercepted phone call from the morning of March 17, 2010 and the subsequent surveillance provided probable cause to believe that evidence of criminal activity would be found in the vehicle.

b. Legal Standard

"[A]ll that is required to stop and search an automobile on the highway is probable cause to believe that it contains any type of contraband." *United States v. Azhocar*, 581 F.2d 735, 737 (9th Cir. 1978); *United States v. Brooks*, 610 F.3d 1186, 1193 (9th Cir. 2010) ("police may conduct a warrantless search of a vehicle if there is probable cause to believe that the vehicle contains evidence of a crime"). The Supreme Court defines probable cause as "a fair probability that contraband will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238 (1983). *Gates* emphasized that "'only the probability, and not a prima

facie showing, of criminal activity is the standard of probable cause." *Id*. at 235 (quoting *Spinelli v. United States*, 393 U.S. 410, 419 (1969)). This assessment is based on "the collective knowledge of all the officers involved in the criminal investigation [even if] all of the information known to the law enforcement officers involved in the investigation is not communicated to the officer who actually [undertakes the challenged action]." *United States v. Ramirez*, 473 F.3d 1026, 1032 (9th Cir. 2007) (internal quotation marks omitted).

c. Ruling of the Court

In this case, the government agents intercepted phone calls between Defendant Madrid and others indicating Defendant Madrid was involved in drug trafficking between the United States and Mexico. On March 17, 2010, agents intercepted a call indicating Defendant Madrid would be transporting contraband later that day. Government agents observed Defendant Madrid arrive at a residence, park in a closed garage, and then leave shortly after driving southbound towards Mexico. The Court concludes that the government agents had probable cause to believe that Defendant Madrid's vehicle contained contraband or evidence of criminal activity. The Government had probable cause to stop and search Madrid's vehicle.

CONCLUSION

IT IS HEREBY ORDERED that (1) the Motion to Suppress Wiretap Evidence and to Order the Government to Issue a Bill of Particulars (ECF No. 57) is DENIED; (2) the Motion to Suppress Evidence (ECF No. 69) is DENIED and (3) the Amended Motion to Suppress (ECF No. 78) is denied.

DATED: May 24, 2012

/s/ William Q. Hayes
WILLIAM Q. HAYES
United Sates District Judge

APPENDIX E

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA v. MICHAEL CAREY (1)	**JUDGMENT IN A CRIMINAL CASE** (For Offenses Committed On or After November 1, 1987) Case Number: 11CR0671-WQH JAN RONIS, RET Defendant's Attorney

REGISTRATION NO. 25751298

☐

THE DEFENDANT:

☒ pleaded guilty to count(s)
1 OF THE INDICTMENT

☐ was found guilty on count(s)
_____ after a plea of not guilty.

Accordingly, the defendant is adjudged guilty of such count(s), which involve the following offense(s):

Title & Section	**Nature of Offense**	**Count Number(s)**
21 USC 846, 841(a)(1)	CONSPIRACY TO DISTRIBUTE COCAINE	1

The defendant is sentenced as provided in pages 2 through 4 of this judgment. The sentence is imposed pursuant to the Sentencing Reform Act of 1984.

☐ The defendant has been found not guilty on count(s) _____

☐ Count(s) _____ is ☐ are ☐ dismissed on the motion of the United States.

☒ Assessment: $100.00

☒ Fine waived ☐ Forfeiture pursuant to order filed _____, included herein.

IT IS ORDERED that the defendant shall notify the United States Attorney for this district within 30 days of any change of name, residence, or mailing address until all fines, restitution, costs, and special assessments imposed by this judgment are fully paid. If ordered to pay restitution, the defendant shall notify the court and United States Attorney of any material change in the defendant's economic circumstances.

APRIL 23, 2014
Date of Imposition of Sentence

/s/ William Q. Hayes
HON. WILLIAM Q. HAYES
UNITED STATES DISTRICT JUDGE

IMPRISONMENT

The defendant is hereby committed to the custody of the United States Bureau of Prisons to be imprisoned for a term of 150 months

☐ Sentence imposed pursuant to Title 8 USC Section 1326(b).

☒ The court makes the following recommendations to the Bureau of Prisons:

That the defendant be designated to a facility in the Western Region and participate in the Residential Drug Abuse Program (RDAP)

☐ The defendant is remanded to the custody of the United States Marshal.

☐ The defendant shall surrender to the United States Marshal for this district:

☐ at _____ ☐ a.m. ☐ p.m. on _____

as notified by the United States Marshal.

☐ The defendant shall surrender for service of sentence at the institution designated by the Bureau of Prisons:

☐ before _____

☐ as notified by the United States Marshal,

☐ as notified by the Probation or Pretrial Services Office.

RETURN

I have executed this judgment as follows:

Defendant delivered on _____ to _____ at _____, with a certified copy of this judgment.

_____
UNITED STATES MARSHAL

By _____
DEPUTY UNITED STATES MARSHAL

SUPERVISED RELEASE

Upon release from imprisonment, the defendant shall be on supervised release for a term of: 5 years

The defendant shall report to the probation office in the district to which the defendant is released within 72 hours of release from the custody of the Bureau of Prisons.

The defendant shall not commit another federal, state or local crime.

For offenses committed on or after September 13, 1994:

The defendant shall not illegally possess a controlled substance. The defendant shall refrain from any unlawful use of a controlled substance. The defendant shall submit to one drug test within 15 days of release from imprisonment and at least two periodic drug tests thereafter as determined by the court. Testing requirements will not exceed submission of more than 4 drug tests per month during the term of supervision, unless otherwise ordered by court.

☐ The above drug testing condition is suspended, based on the court's determination that the defendant poses a low risk of future substance abuse. (Check, if applicable.)

☒ The defendant shall not possess a firearm, ammunition, destructive device, or any other dangerous weapon.

☒ The defendant shall cooperate in the collection of a DNA sample from the defendant, pursuant to section 3 of the DNA Analysis Backlog Elimination Act of 2000, pursuant to 18 USC, sections 3563(a)(7) and 3583(d).

☐ The defendant shall comply with the requirements of the Sex Offender Registration and Notification Act (42 U.S.C. § 16901, et seq.) as directed by the probation officer, the Bureau of Prisons, or any state sex offender registration agency in which he or she resides, works, is a student, or was convicted of a qualifying offense. (Check if applicable.)

☐ The defendant shall participate in an approved program for domestic violence. (Check, if applicable.)

If this judgment imposes a fine or restitution obligation, it is a condition of supervised release that the defendant pay any such fine or restitution that remains unpaid at the commencement of the term of supervised release in accordance with the Schedule of Payments set forth in this judgment.

The defendant must comply with the standard conditions that have been adopted by this court. The defendant shall also comply with any special conditions imposed.

STANDARD CONDITIONS OF SUPERVISION

1) the defendant shall not leave the judicial district without the permission of the court or probation officer;

2) the defendant shall report to the probation officer in a manner and frequency directed by the court or probation officer;

3) the defendant shall answer truthfully all inquiries by the probation officer and follow the instructions of the probation officer;

4) the defendant shall support his or her dependents and meet other family responsibilities;

5) the defendant shall work regularly at a lawful occupation, unless excused by the probation officer for schooling, training, or other acceptable reasons;

6) the defendant shall notify the probation officer at least ten days prior to any change in residence or employment;

7) the defendant shall refrain from excessive use of alcohol and shall not purchase, possess, use, distribute, or administer any controlled substance or any paraphernalia related to any controlled substances, except as prescribed by a physician;

8) the defendant shall not frequent places where controlled substances are illegally sold, used, distributed, or administered;

9) the defendant shall not associate with any persons engaged in criminal activity and shall not associate with any person convicted of a felony, unless granted permission to do so by the probation officer;

10) the defendant shall permit a probation officer to visit him or her at any time at home or elsewhere and shall permit confiscation of any contraband observed in plain view of the probation officer;

11) the defendant shall notify the probation officer within seventy-two hours of being arrested or questioned by a law enforcement officer;

12) the defendant shall not enter into any agreement to act as an informer or a special agent of a law enforcement agency without the permission of the court; and

13) as directed by the probation officer, the defendant shall notify third parties of risks that may be occasioned by the defendant's criminal record or personal history or characteristics and shall permit the probation officer to make such notifications and to confirm the defendant's compliance with such notification requirement.

SPECIAL CONDITIONS OF SUPERVISION

☒ Submit person, property residence, office or vehicle to a search, conducted by a United States Probation Officer at a reasonable time and in a reasonable manner, based upon reasonable suspicion of contraband or evidence of a violation of a condition of release; failure to submit to a search may be grounds for revocation; the defendant shall warn any other residents that the premises may be subject to searches pursuant to t

☐ If deported, excluded, or allowed to voluntarily return to country of origin, not reenter the United States illegally and report to the probation officer within 24 hours of any reentry to the United States; supervision waived upon deportation, exclusion or voluntary departure.

☐ Not transport, harbor, or assist undocumented aliens.

☐ Not associate with undocumented aliens or alien smugglers.

☐ Not reenter the United States illegally.

☒ Not enter or reside in the Republic of Mexico without written permission of the Court or probation officer.

☒ Report all vehicles owned or operated, or in which you have an interest, to the probation officer.

☐ Not possess any narcotic drug or controlled substance without a lawful medical prescription.

☐ Not associate with known users of, smugglers of, or dealers in narcotics, controlled substances, or dangerous drugs in any form.

☐ Participate in a program of mental health treatment as directed by the probation officer. The Court authorizes the release of the presentence report and available psychological evaluations to the mental health provider, as approved by the probation officer. Allow for reciprocal release of information between the probation officer and the treatment provider. May be required to contribute to the costs of services rendered in an amount to be determined by the probation officer, based on the defendant's ability to pay.

☐ Take no medication containing a controlled substance without valid medical prescription, and provide proof of prescription to the probation officer, if directed.

☐ Provide complete disclosure of personal and business financial records to the probation officer as requested.

☐ Be prohibited from opening checking accounts or incurring new credit charges or opening additional lines of credit without approval of the probation officer.

☐ Seek and maintain full time employment and/or schooling or a combination of both.

☐ Resolve all outstanding warrants within days.

☐ Complete hours of community service in a program approved by the probation officer within

☐ Reside in a Residential Reentry Center (RRC) as directed by the probation officer for a period of

☐ Participate in a program of drug or alcohol abuse treatment, including urinalysis or sweat patch testing and counseling, as directed by the probation officer. Allow for reciprocal release of information between the probation officer and the treatment provider. May be required to contribute to the costs of services rendered in an amount to be determined by the probation officer, based on the defendant's ability to pay.

APPENDIX F

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA, Plaintiff-Appellee, v. MICHAEL CAREY, AKA Garrocha, Defendant-Appellant.	No. 18-50393 D.C. No. 3: 11-cr-00671-WQH-1 Southern District of California, San Diego ORDER May 18, 2023

Before: WALLACE, HURWITZ, and BADE, Circuit Judges.

Judge Bade voted to deny the petition for rehearing en banc. Judges Wallace and Hurwitz recommended denying it.

The full court has been advised of the petition for rehearing en banc and no judge has requested a vote on whether to rehear the matter en banc. Fed. R. App. P. 35.

The petition for rehearing en banc, Dkt. 113, is **DENIED**.

APPENDIX G

CONSTITUTIONAL AND STATUTORY PROVISIONS INVOLVED

U.S. Const. amend. IV.

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

18 U.S.C. § 2510. 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]

(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;

---

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

(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;

(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.

18 U.S.C. § 2511. Interception and disclosure of wire, oral, or electronic communications prohibited

(1) Except as otherwise specifically provided in this chapter any person who—

(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;

(b) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when—

(i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or

(ii) such device transmits communications by radio, or interferes with the transmission of such communication; or

(iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or

(iv) such use or endeavor to use (A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or

(v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States;

(c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;

(d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; or

(e)(i) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, intercepted by means authorized by sections 2511(2)(a)(ii), 2511(2)(b)–(c), 2511(2)(e), 2516, and 2518 of this chapter, (ii) knowing or having reason to know that the information was obtained through the interception of such a communication in connection with a criminal investigation, (iii) having obtained or received the information in connection with a criminal investigation, and (iv) with intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation,

shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

(2)(a)(i) It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to

intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

(ii) Notwithstanding any other law, providers of wire or electronic communication service, their officers, employees, and agents, landlords, custodians, or other persons, are authorized to provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, if such provider, its officers, employees, or agents, landlord, custodian, or other specified person, has been provided with—

(A) a court order directing such assistance or a court order pursuant to section 704 of the Foreign Intelligence Surveillance Act of 1978 signed by the authorizing judge, or

(B) a certification in writing by a person specified in section 2518(7) of this title or the Attorney General of the United States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required,

setting forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required. No provider

of wire or electronic communication service, officer, employee, or agent thereof, or landlord, custodian, or other specified person shall disclose the existence of any interception or surveillance or the device used to accomplish the interception or surveillance with respect to which the person has been furnished a court order or certification under this chapter, except as may otherwise be required by legal process and then only after prior notification to the Attorney General or to the principal prosecuting attorney of a State or any political subdivision of a State, as may be appropriate. Any such disclosure, shall render such person liable for the civil damages provided for in section 2520. No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of a court order, statutory authorization, or certification under this chapter.

(iii) If a certification under subparagraph (ii)(B) for assistance to obtain foreign intelligence information is based on statutory authority, the certification shall identify the specific statutory provision and shall certify that the statutory requirements have been met.

(b) It shall not be unlawful under this chapter for an officer, employee, or agent of the Federal Communications Commission, in the normal course of his employment and in discharge of the monitoring responsibilities exercised by the Commission in the enforcement of chapter 5 of title 47 of the United States Code, to intercept a wire or electronic communication, or oral communication transmitted by radio, or to disclose or use the information thereby obtained.

(c) It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.

(d) It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

(e) Notwithstanding any other provision of this title or section 705 or 706 of the Communications Act of 1934, it shall not be unlawful for an officer, employee, or agent of the United States in the normal course of his official duty to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act.

(f) Nothing contained in this chapter or chapter 121 or 206 of this title, or section 705 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, and procedures in this chapter or chapter 121 and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive

means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted.

(g) It shall not be unlawful under this chapter or chapter 121 of this title for any person—

(i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public;

(ii) to intercept any radio communication which is transmitted—

(I) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress;

(II) by any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public;

(III) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or

(IV) by any marine or aeronautical communications system;

(iii) to engage in any conduct which—

(I) is prohibited by section 633 of the Communications Act of 1934; or

(II) is excepted from the application of section 705(a) of the Communications Act of 1934 by section 705(b) of that Act;

(iv) to intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of such interference; or

(v) for other users of the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled or encrypted.

(h) It shall not be unlawful under this chapter—

(i) to use a pen register or a trap and trace device (as those terms are defined for the purposes of chapter 206 (relating to pen registers and trap and trace devices) of this title); or

(ii) for a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful or abusive use of such service.

(i) It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer, if—

(I) the owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer;

(II) the person acting under color of law is lawfully engaged in an investigation;

(III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and

(IV) such interception does not acquire communications other than those transmitted to or from the computer trespasser.

(j) It shall not be unlawful under this chapter for a provider of electronic communication service to the public or remote computing service to intercept or disclose the contents of a wire or electronic communication in response to an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies section 2523.

(3)(a) Except as provided in paragraph (b) of this subsection, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

(b) A person or entity providing electronic communication service to the public may divulge the contents of any such communication—

(i) as otherwise authorized in section 2511(2)(a) or 2517 of this title;

(ii) with the lawful consent of the originator or any addressee or intended recipient of such communication;

(iii) to a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or

(iv) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.

(4)(a) Except as provided in paragraph (b) of this subsection or in subsection (5), whoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both.

(b) Conduct otherwise an offense under this subsection that consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled and that is transmitted—

(i) to a broadcasting station for purposes of retransmission to the general public; or

(ii) as an audio subcarrier intended for redistribution to facilities open to the public, but not including data transmissions or telephone calls,

is not an offense under this subsection unless the conduct is for the purposes of direct or indirect commercial advantage or private financial gain.

(5)(a)(i) If the communication is—

(A) a private satellite video communication that is not scrambled or encrypted and the conduct in violation of this chapter is the private

viewing of that communication and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain; or

(B) a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct in violation of this chapter is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain,

then the person who engages in such conduct shall be subject to suit by the Federal Government in a court of competent jurisdiction.

(ii) In an action under this subsection—

(A) if the violation of this chapter is a first offense for the person under paragraph (a) of subsection (4) and such person has not been found liable in a civil action under section 2520 of this title, the Federal Government shall be entitled to appropriate injunctive relief; and

(B) if the violation of this chapter is a second or subsequent offense under paragraph (a) of subsection (4) or such person has been found liable in any prior civil action under section 2520, the person shall be subject to a mandatory $500 civil fine.

(b) The court may use any means within its authority to enforce an injunction issued under paragraph (ii)(A), and shall impose a civil fine of not less than $500 for each violation of such an injunction.

18 U.S.C. § 2512. Manufacture, distribution, possession, and advertising of wire, oral, or electronic communication intercepting devices prohibited

(1) Except as otherwise specifically provided in this chapter, any person who intentionally—

(a) sends through the mail, or sends or carries in interstate or foreign commerce, any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications;

(b) manufactures, assembles, possesses, or sells any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications, and that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce; or

(c) places in any newspaper, magazine, handbill, or other publication or disseminates by electronic means any advertisement of—

(i) any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications; or

(ii) any other electronic, mechanical, or other device, where such advertisement

promotes the use of such device for the purpose of the surreptitious interception of wire, oral, or electronic communications,

knowing the content of the advertisement and knowing or having reason to know that such advertisement will be sent through the mail or transported in interstate or foreign commerce,

shall be fined under this title or imprisoned not more than five years, or both.

(2) It shall not be unlawful under this section for—

(a) a provider of wire or electronic communication service or an officer, agent, or employee of, or a person under contract with, such a provider, in the normal course of the business of providing that wire or electronic communication service, or

(b) an officer, agent, or employee of, or a person under contract with, the United States, a State, or a political subdivision thereof, in the normal course of the activities of the United States, a State, or a political subdivision thereof,

to send through the mail, send or carry in interstate or foreign commerce, or manufacture, assemble, possess, or sell any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications.

(3) It shall not be unlawful under this section to advertise for sale a device described in subsection (1) of this section if the advertisement is mailed, sent, or carried in interstate or foreign commerce solely to a domestic provider of wire or electronic communication

service or to an agency of the United States, a State, or a political subdivision thereof which is duly authorized to use such device.

18 U.S.C. § 2513. Confiscation of wire, oral, or electronic communication intercepting devices

Any electronic, mechanical, or other used, sent, carried, manufactured, assembled, possessed, sold, or advertised in violation of section 2511 or section 2512 of this chapter may be seized and forfeited to the United States. All provisions of law relating to (1) the seizure, summary and judicial forfeiture, and condemnation of vessels, vehicles, merchandise, and baggage for violations of the customs laws contained in title 19 of the United States Code, (2) the disposition of such vessels, vehicles, merchandise, and baggage or the proceeds from the sale thereof, (3) the remission or mitigation of such forfeiture, (4) the compromise of claims, and (5) the award of compensation to informers in respect of such forfeitures, shall apply to seizures and forfeitures incurred, or alleged to have been incurred, under the provisions of this section, insofar as applicable and not inconsistent with the provisions of this section; except that such duties as are imposed upon the collector of customs or any other person with respect to the seizure and forfeiture of vessels, vehicles, merchandise, and baggage under the provisions of the customs laws contained in title 19 of the United States Code shall be performed with respect to seizure and forfeiture of electronic, mechanical, or other intercepting devices under this section by such officers, agents, or other persons as may be authorized or designated for that purpose by the Attorney General.

18 U.S.C. § 2515. 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.

18 U.S.C. § 2518. 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.

18 U.S.C. § 2520. Recovery of civil damages authorized

(a) IN GENERAL.—Except as provided in section 2511(2)(a)(ii), any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a

civil action recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.

(b) RELIEF.—In an action under this section, appropriate relief includes—

(1) such preliminary and other equitable or declaratory relief as may be appropriate;

(2) damages under subsection (c) and punitive damages in appropriate cases; and

(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

(c) COMPUTATION OF DAMAGES.—(1) In an action under this section, if the conduct in violation of this chapter is the private viewing of a private satellite video communication that is not scrambled or encrypted or if the communication is a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, then the court shall assess damages as follows:

(A) If the person who engaged in that conduct has not previously been enjoined under section 2511(5) and has not been found liable in a prior civil action under this section, the court shall assess the greater of the sum of actual damages suffered by the plaintiff, or statutory damages of not less than $50 and not more than $500.

(B) If, on one prior occasion, the person who engaged in that conduct has been enjoined under section 2511(5) or has been found liable in a civil

action under this section, the court shall assess the greater of the sum of actual damages suffered by the plaintiff, or statutory damages of not less than $100 and not more than $1000.

(2) In any other action under this section, the court may assess as damages whichever is the greater of—

(A) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or

(B) statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000.

(d) DEFENSE.—A good faith reliance on—

(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;

(2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or

(3) a good faith determination that section 2511(3), 2511(2)(i), or 2511(2)(j) of this title permitted the conduct complained of;

is a complete defense against any civil or criminal action brought under this chapter or any other law.

(e) LIMITATION.—A civil action under this section may not be commenced later than two years after the date upon which the claimant first has a reasonable opportunity to discover the violation.

(f) ADMINISTRATIVE DISCIPLINE.—If a court or appropriate department or agency determines that the United States or any of its departments or agencies

has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.

(g) IMPROPER DISCLOSURE IS VIOLATION.—Any willful disclosure or use by an investigative or law enforcement officer or governmental entity of information beyond the extent permitted by section 2517 is a violation of this chapter for purposes of section 2520(a).

18 U.S.C. § 2521. Injunction against illegal interception

Whenever it shall appear that any person is engaged or is about to engage in any act which constitutes or will constitute a felony violation of this chapter, the Attorney General may initiate a civil action in a district court of the United States to enjoin such violation. The court shall proceed as soon as practicable to the hearing and determination of such an action, and may, at any time before final determination, enter such a restraining order or prohibition, or take such other action, as is warranted to prevent a continuing

and substantial injury to the United States or to any person or class of persons for whose protection the action is brought. A proceeding under this section is governed by the Federal Rules of Civil Procedure, except that, if an indictment has been returned against the respondent, discovery is governed by the Federal Rules of Criminal Procedure.