# THE GOVERNMENT HAD MY WIRES TAPPED: Litigating Title III Wiretaps

## NACDL Spring Meeting & Seminar
## Search, Seizure & Criminal Litigation

**April 18-21, 2018**
**New York City**

# A TITLE III (WIRETAP) PRIMER

Steven Kalar, Federal Public Defender
Northern District of California
Josh A. Cohen
Clarence, Dyer & Cohen, LLP
Gail Shifman
Law Office of Gail Shifman

> The evil incident to invasion of the privacy of the telephone is far greater than that involved in tampering with the mails. Whenever a telephone line is tapped, the privacy of the persons at both ends of the line is invaded, and all conversations between them upon any subject, and although proper, confidential, and privileged, may be overheard. Moreover, the tapping of one man's telephone line involves the tapping of the telephone of every other person whom he may call, or who may call him. As a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wire tapping.

*Olmstead v. United States*, 277 U.S. 438, 475-76 (1928) (Brandeis, J., dissenting).

> Few threats to liberty exist which are greater than that posed by the use of eavesdropping devices. Some may claim that without the use of such devices crime detection in certain areas may suffer some delays since eavesdropping is quicker, easier, and more certain. However, techniques and practices may well be developed that will operate just as speedily and certainly and – what is more important – without attending illegality.

*Berger v. New York*, 388 U.S. 41, 63 (1967).

## Table of Contents

## Introduction

The number of federal and state wiretaps reported in 2016 decreased 24 percent from 2015. A total of 3,168 wiretaps were reported as authorized in 2016, with 1,551 authorized by federal judges and 1,617 authorized by state judges.[1] Compared to the applications approved during 2015, the number approved by federal judges increased 11 percent in 2016, and the number approved by state judges decreased 41 percent. The largest reduction in reported state wiretap applications occurred in California, where 50 percent fewer applications were reported. Though one might expect a respectable percentage of these applications to be denied, she would be wrong: of the 3,168 applications submitted to the courts last year, exactly two were denied. *Id.*

Despite the decrease in the number of wiretaps authorized in 2016 from 2015, which had 4,148 authorized, the highest number of wiretaps ever, authorized intercept applications reported by year have increased 72 percent from 1,839 in 2006 to the 3,168 approved in 2016. *Id.* Of the more than 32,000 wiretap applications submitted from 2006 through 2016, all but nine were approved. *Id. No wiretap applications were denied in 2006, 2007, 2008, 2009 and 2015. Id.*

Consistent with these trends, defendants are increasingly facing charges generated by electronic interceptions, or "wiretaps." This outline will give a general overview of the federal statutes controlling wiretaps, primarily known as "Title III." It will then discuss four primary defenses available in wiretap litigation:

- "Technical" violations
- "Necessity" shortcomings
- Probable cause shortcomings
- *Franks* challenges

Finally, the outline closes with some general pointers about wiretap litigation. Note that the outline does not focus on the wiretap provisions of the US PATRIOT Act, except where the new law impacts traditional Title III wiretaps for non-terrorism cases.

---

1 *See,* Administrative Office of the U.S. Courts, *Wiretap Report 2016*, Table 7.

## I. LEGISLATIVE HISTORY OF TITLE III

The predecessor to the modern federal wiretap statutory scheme was the Federal Communications Act of 1934, 47 U.S.C. § 605 (1970). *See United States v. Jones*, 542 F.2d 661, & n.10. In the late Sixties, dissatisfaction with this Act, academic criticism, and the reports of scholarly committees drove Congress to create a new wiretap statute: the Omnibus Crime Control and Safe Streets Act of 1968.

One important factor in the creation of the 1968 Act was a series of contemporaneous Supreme Court decisions addressing the constitutionality of wiretapping.[2] Foremost among these was the *Berger* decision, where the Court rejected a New York wiretapping statute. *See Berger v. United States*, 388 U.S. 41, 63 (1967). While discussing a pre-Title III wiretap, the Supreme Court emphasized that "[f]ew threats to liberty exist which are greater than that posed by the use of eavesdropping devices." *Id.* at 63. The Court in *Berger* went on to recognize that although wiretapping is a more expedient form of investigation, expediency in law enforcement must ultimately yield to the requirements of the Fourth Amendment "before the innermost secrets of one's home or office are invaded." *Id.*; *see also United States v. Kalustian*, 529 F.2d 585, 589 (9th Cir. 1976).

The wiretap provisions of the Omnibus Crime Control and Safe Streets Act of 1968 are now codified at 18 USC §§ 2510 - 2520. Because the electronic intercept statutes are found in the third title of the 1968 Act, "Title III" has become a common shorthand for federal wiretaps and wiretap litigation.

Given today's wildly expanding tolerance for wiretapping, it is remarkable to recall that

---

[2] *See, e.g., United States v. Martinez*, 498 F.2d 464, 468 (6th Cir. 1974) ("Though the New York 'Eavesdropping Law' was held unconstitutional in *Berger v. New York*, 388 U.S. 41, 87 S.Ct. 1873, 18 L.Ed.2d 1040 (1967), in pointing out the deficiencies of the New York statute the Court indicated the requirements for a constitutional electronic surveillance law. It is clear that Congress gave careful consideration to the opinions in *Osborn*, *Berger* and *Katz* in drafting 18 USC §§ 2510-2520, Title III of the Omnibus Crime Control and Safe Streets Act of 1968.")

in enacting Title III in 1968, Congress actually intended to *increase* protections for individuals against surveillance and recording. This goal was summarized in one Senate Report:

> Title III has as its dual purpose (1) protecting the privacy of wire and oral communications, and (2) delineating on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized. To assure the privacy of oral and wire communications, Title III prohibits all wiretapping and electronic surveillance by persons other than duly authorized law enforcement officers engaged in the investigation or prevention of specified types of serious crimes, and only after authorization of a court order obtained after a showing and finding of probable cause.

*Jones*, 542 F.2d at 668, quoting S.Rep. No. 1097, *reprinted in* U.S. Code Cong. & Admin. News 1968, 90th Cong., 2d Sess., at 2153.

Like many federal statutes, Title III is cobbled together from competing draft legislation originating in the House and Senate.[3] Controversial terms – like who exactly can authorize a

[3] *See generally United States v. Giordano*, 416 U.S. 505, 518 & n. 7 (1974) ("In 1967, a draft statute prepared by Professor G. Robert Blakey of the University of Notre Dame Law School to regulate the interception of wire and oral communications was published in The President's Commission on Law Enforcement and Administration of Justice, Task Force Report: Organized Crime, Appendix C, at 106 – 113. In part, it would have added a provision to Title 18, United States Code, which empowered the 'Attorney General or any Assistant Attorney General of the Department of Justice specially designated by the Attorney General' to authorize an application to a federal judge for an order to intercept wire or oral communications. *Id.* at 108. Senator McClellan introduced a proposed 'Federal Wire Interception Act,' S. 675, on January 25, 1967, 113 Cong.Rec. 1491 containing, in § 5(a), the same designations of which federal prosecuting officials could authorize a wiretap application. Hearings on Controlling Crime Through More Effective Law Enforcement before the Subcommittee on Criminal Laws and Procedures of the Senate Committee on the Judiciary, 90th Cong., 1st Sess., 76 (1967). Senator Hruska later introduced S. 2050 on June 29, 1967, 113 Cong.Rec. 18007, which would have provided for regulated use of electronic surveillance, as well as wiretapping, and which again made provision, in a new § 2516 to be added to Title 18, United States Code, for the same system of approval of applications for the interception of wire or oral communications as was present in the Blakey bill. Hearings, *supra*, at 1005. In the House of Representatives, the Blakey bill was introduced on October 3, 1967, in the form of H.R. 13275, 113 Cong.Rec. 27718. Ultimately, the same operative language was enacted in Title III.")

wiretap application, whether the statute creates a private cause of action, and the like – require exhaustive legislative analysis of the specific subsection. *See generally United States v. Giordano*, 416 U.S. 505, 518 (1974).

## II. INTRODUCTION TO TITLE III CHALLENGES

### A. *Definitions*

An initial hurdle in Title III litigation is the unique wiretap vocabulary. Some of the most common terms are accordingly defined below:

· **Authorizing Court**: This is the district court which originally grants the wiretap applications, and which receives ten-day reports and extension applications. Different courts can handle extension applications, but the information provided to the original court cannot be imputed – each judge must be presented with a full showing of necessity and probable cause.

· **Minimization**: Title III requires that federal agents monitor the intercepted conversations and minimize the calls, to capture only pertinent conversations. 18 U.S.C. § 2518(5) (requiring that wiretaps be conducted in such a way as to "minimize the interception of communications not otherwise subject to interception under this chapter . . . .") The Supreme Court has explained that the "minimization" requirement involves a contextual analysis. *See United States v. Scott*, 436 U.S. 128, 140 (1978) ("The statute does not forbid the interception of all nonrelevant conversations, but rather instructs the agents to conduct the surveillance in such a manner as to 'minimize' the interception of such conversations. Whether the agents have in fact conducted the wiretap in such a manner will depend on the facts and circumstances of each case.")

· **Monitoring Logs**: Agents monitor calls during the interception, both to detect criminal activity and to comply with Title III minimization requirements. Monitoring logs from older wiretaps had handwritten agents' notes; most modern wiretaps will have electronic monitoring logs with entries that correspond to a name assigned to the intercepted call.

· **Necessity:** "Necessity" in the Title III context refers to the government's showing that the goal of the investigation could not be achieved through normal investigative techniques – thus, the wiretap was necessary. *See* 18 U.S.C. § 2518(3)(c)(3) ("Upon such application the judge may enter an *ex parte order* . . . authorizing . . . interception of . . . electronic

communications . . . if the judge determines on the basis of the facts submitted by the applicant 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."). Title III necessity shortcomings are one of the key defense challenges to a wiretap.

· **Pen register:** Pen register devices capture only the "numbers dialed or otherwise transmitted" on the telephone line to which the device is attached. 18 USC § 3127(3). In other words, a pen register keeps track of the numbers dialed from the target number.

· **"Re-up" or "Extension" Applications:** A federal wiretap order can only authorize interceptions for thirty days. After thirty days, the government must apply for an extension, or "re-up" application. *See* 18 USC § 2518(5) ("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.")

· **Reviewing Court**: This is the district court that reviews the legality of the wiretap in response to a defense challenge. It often is a different district court judge than the authorizing court, but there is no legal bar to the authorizing court reviewing its own authorizations.

· **Target Number:** The phone number that will be tapped, trapped and traced, or upon which a pen register will be installed.

· **Title III**: As noted *supra*, this refers to Title III of the Omnibus Crime Control and Safe Streets Act of 1968 – the controlling federal wiretap statute. It is a common shorthand for federal wiretap law and challenges.

· **Trap and Trace**: "[A] device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication." 18 USC § 3127(4). Essentially, technology that will identify the *number calling* the target number.

· **Toll register:** Essentially, a phone bill. This is provided by the phone company, and

tracks the numbers called and the duration of the call. Often obtained by federal agencies before a wiretap.

### B. *Standards of Review*

A wiretap challenge in the district court is, essentially, appellate review of the original authorizing court's decision to permit a wiretap. The standard of review varies widely depending on the legal issue raised – a facial attack is reviewed for abuse of discretion[4], while a *Franks* challenge is *de novo.*[5] These standards of review are discussed briefly below.

An interesting issue is whether the reviewing *district* court applies the same standards of review articulated in *appellate (Circuit)* decisions. While there are few decisions addressing the issue, at least one district court has held that the same standards apply. *See United States v. Valdez-Pacheco*, 701 F.Supp. 775, 884 (D. Or. 1989).

· **Facial Challenges:** A district court's decision to authorize a wiretap on the *face of the application and affidavit* is reviewed for an abuse of discretion. *See United States v. Canales Gomez*, 358 F.3d 1221, 1225 (9th Cir. 2004); *United States v. Blackmon*, 273 F.3d 1204, 1207 (9th Cir. 2001); *United States v. Echavarria-Olarte*, 904 F.2d 1391, 1395 (9th Cir. 1990); *United States v. Carneiro*, 861 F.2d 1171, 1177 (9th Cir. 1988).

· **Did the Government Comply with Sealing Requirements?:** The district court's determination that the government did not violate Title III sealing requirements is reviewed *de novo*. *United States v. McGuire*, 307 F.3d 1192, 1203 (2002) ("McGuire argues that the recordings were not sealed 'immediately' upon the expiration of the order authorizing wiretapping and that there was no satisfactory explanation for the delay. The district court's determination that the government did not violate Title III is reviewed *de novo*.")

· **Did the Government's Application Provide a "Full and Complete Statement"?:** The authorizing court's determination that the government's wiretap application complied with the "full and complete statement" requirement of Section 2518(1)(c) is reviewed *de novo*. *See United States v. Blackmon*, 273 F.3d 1204, 1207 (9th Cir. 2001); *United States v. Brone*, 792

---

[4] *See United States v. Canales Gomez*, 358 F.3d 1221, 1225 (9th Cir. 2004)

[5] *See United States v. Elliott*, 893 F.2d 220, 222 (9th Cir. 1990).

F.2d 1504, 1506 (9th Cir. 1986). *United States v. Rodriguez, 851 F.3d 931, 942 (9th Cir. 2017),* where the Court concluded that district courts should apply the two-step approach when considering a motion to suppress wiretap evidence, first conducting a de novo review as to whether the application contains a full and complete statement as to whether or not other investigative procedures have been tried and failed or whey they reasonably appear to be unlikely to succeed if tried or to be too dangerous and if the application meets these requirements, then the district court judge should review for abuse of discretion the issuing judge's conclusion that the wiretap was necessary.

· **The "Necessity" for the Wiretap *Without Franks* Errors:** The authorizing court's finding of necessity may be overturned only for abuse of discretion. *United States v. Bennett*, 219 F.3d 1117, 1121 (9th Cir. 2000). *But* whether other investigative procedures have been exhausted or why they reasonably appear not likely to succeed is reviewed *de novo*. *United States v. Lynch*, 367 F.3d 1148, 1159 (9th Cir. 2004). In *Brone*, the Ninth Circuit explained, "We review *de novo* whether a full and complete statement of the facts was submitted in compliance with 18 USC § 2518(1)(c), but we review the issuing judge's decision that the wiretaps were necessary for an abuse of discretion." *United States v. Brone*, 792 F.2d 1504, 1506 (9th Cir. 1986); *see also Canales Gomez*, 358 F.3d at 1224 (stating that a court must review *de novo* whether the requisite full and complete statement of facts was submitted in compliance with 18 USC § 2518(1)(c)); *United States v. Shryock*, 342 F.3d 948, 975 (9th Cir. 2003), *cert. denied*, 124 S. Ct. 1729 (2004) (same); *United States v. McGuire*, 307 F.3d 1192, 1197 (9th Cir. 2002) (same); *Blackmon*, 273 F.3d at 1207 (same); *Carneiro*, 861 F.2d at 1176 (same).

· **Probable Cause Affected by *Franks* Omissions:** The reviewing court should conduct a *de novo* review of the original decisions to authorize the interceptions. *See United States v. Elliott*, 893 F.2d 220, 222 (9th Cir. 1990). As the Ninth Circuit observed in *Elliott*, *de novo* review is appropriate because the probable cause question "turns on the consequences of a fraud on the issuing magistrate which that magistrate was not in a position to evaluate." *Id.*

· **Denial of *Franks* Hearing, and Underlying Factual Findings:** "We review the district court's denial of a *Franks* hearing *de novo*, and we review underlying factual findings

for clear error. *United States v. Shyrock*, 342 F.3d 948, 975 (9th Cir. 2003)." *United States v. Staves*, 383 F.3d 977, 980 (9th Cir. 2004).

· **Are *Franks* Omissions or False Statements Essential to P.C. or Necessity?**: The ultimate question whether a false statement or omission is essential to a finding of probable cause or necessity is a mixed question of law and fact reviewed *de novo*. *United States v. Tham*, 960 F.2d 1391, 1395 (9th Cir. 1992).

### C. *Challenging Wiretap Applications and Orders Within Their Four Corners*

A wiretap challenge is an intensely fact-bound analysis that turns upon the language of a particular application and affidavit. Therefore, a defense challenge should analyze each separate application (and supporting affidavit) in turn.[6] *See, e.g., United States v. Carneiro*, 861 F.2d 1171, 1176 (9th Cir. 1988) ("The district court erred in failing to examine each wiretap application separately. *Each* wiretap application, standing alone, must satisfy the necessity requirement.").

Moreover, when defending the wiretap applications and orders, the government must be limited to the facts and information contained within the application and affidavits when presented to the authorizing court. *See, e.g., United States v. Meling*, 47 F.3d 1546, 1551-52 (9th Cir. 1995) ("*Looking only to the four corners of the wiretap application*, we will uphold the wiretap if there is a substantial basis for these findings of probable cause.") (emphasis added). Note, however, that the government can incorporate testimony or affidavits by reference in the application (as long as these documents are physically before the authorizing court).

### D. *No "Good Faith" (Leon) Exceptions*

It has not been directly decided whether the *Leon* "good faith" exception applies to wiretaps. There are, however, compelling arguments against the importation of *Leon* into Title III litigation.

There are two layers of protections available to those subject to federal wiretaps: the Fourth Amendment, and the statutory requirements of Title III. *See United States v. Donovan*,

[6] A motion seeking suppression of information from the wiretap must be brought before trial. *See* 18 USC § 2518(10)(a).

429 U.S. 413, 432 n.22 (1977) ("The availability of the suppression remedy [for Title III], as opposed to constitutional, violations. . . turns on the provisions of Title III rather than the judicially fashioned exclusionary rule aimed at deterring violations of Fourth Amendment rights."). Because wiretap law is statutory, and Fourth Amendment exclusionary rules are court-created, federal courts cannot import Fourth Amendment exclusion exceptions into Title III suppression remedies – including the *Leon* "good faith" exception.

In *United States v. Leon,* 468 U.S. 897 (1984), the Supreme Court held that the Fourth Amendment did not require exclusion of evidence obtained by law enforcement officers who acted in reasonable reliance on a search warrant which was issued by a detached and neutral magistrate but was ultimately found to be unsupported by probable cause. As illustrated by *Leon*, federal courts enjoy the freedom to carve exceptions to the court-created Fourth Amendment exclusionary rule. The suppression remedies in Title III, however, were created by Congress – and federal courts cannot alter or limit those remedies.[7] *See, e.g., United States v. Wuliger*, 981 F.2d 1497 (6th Cir. 1992) (refusing to recognize 'impeachment exception' to Title III in civil cases); *United States v. Vest*, 813 F.2d 477, 484 (1st Cir. 1987) ("We therefore

---

[7] The Sixth Circuit has explained how the privacy goals of Title III prevent courts from importing Fourth Amendment exceptions into the wiretap suppression remedy:

> Title III has as its dual purpose (1) protecting the privacy of wire and oral communications, and (2) delineating on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized.
>
> [A]lthough Title III authorizes invasions of individual privacy under certain circumstances, the protection of privacy was an overriding congressional concern. *Fultz v. Gilliam*, 942 F.2d 396, 401 (6th Cir.1991) (citations omitted; emphasis added).
>
> In light of this overriding concern for protection of privacy, and because the Act sets out when certain uses or disclosures of wiretap material are authorized, it may be implied that 'what is not permitted is forbidden.'

*United States v. Wuliger*, 981 F.2d 1497, 1506 (6th Cir. 1992).

decline to read into section 2515 an exception permitting the use of illegally-intercepted communications in perjury prosecutions."); *In Re Grand Jury*, 111 F.3d 1066, 1077-78 (3rd Cir. 1997) (refusing to permit unlawful interceptions, obtained with "clean hands", to be used as evidence in grand jury proceedings).

## III. "TECHNICAL"/"FACIAL" CHALLENGES TO TITLE III ELECTRONIC INTERCEPTIONS

A federal wiretap is a minefield of statutory requirements, and any wiretap deserves close scrutiny to identify any missteps by the government.8 Title III specifically provides that a defendant may move to suppress the fruits of a wire or oral intercept on the grounds that: "(i) the communication was unlawfully intercepted; [or] (ii) the order of authorization or approval under which it was intercepted is insufficient on its face ...." 18 U.S.C. § 2518(10)(a); see also 18 U.S.C. § 2515 (preventing disclosure of wiretap evidence obtained "in violation of this chapter").

"The procedural steps provided in the Act require 'strict adherence.' *United States v. Kalustian*, 529 F.2d 585, 588 (9th Cir.1976) (citing *United States v. Giordano*, 416 U.S. 505, 94 S.Ct. 1820, 40 L.Ed.2d 341 (1974)), and 'utmost scrutiny must be exercised to determine whether wiretap orders conform to Title III.' *Id*. at 589." *Blackmon*, 273 F.3d at 1207. Defense attacks focused on these technical statutory requirements are often called "facial challenges," because they examine the sufficiency of the application on its face – without *Franks* analysis. *See, generally, Giordano*, 416 U.S. 505.

The broad contours of these facial challenges are summarized below:

### A. *Did the Correct DOJ Official Authorize the Application?*

Title III requires that the Attorney General of the Department of Justice, or a properly-designated subordinate, must authorize an AUSA's application for a wiretap. The DOJ official that authorized the wiretap application must be specifically identified in the *application*. 18

[8] *See In re Globe*, 729 F.2d 47, 55 (1st Cir. 1984) ("Title III is an extremely complex statute with whose detailed provisions even the most meticulous law enforcement officer or authorizing judge might inadvertently fail to comply.")

USC § 2518(1). Similarly, the ultimate wiretap *order* must specify the person at DOJ who authorized the application. 18 USC § 2518(4); *see also United States v. Reyna*, 218 F.3d 1108 (9th Cir. 2000) ("Both the application and the court order approving the application must state the identity of the officer authorizing the application.")

These Title III "authorizing official" requirements are set forth in the following chart:

| **Title III Statutory References to Authorized Officials** | | |
|---|---|---|
| **18 USC § 2518(10)(a)(iii) –**<br><br>**Authority permitting challenges based on insufficiency of wiretap order.** | **18 USC § 2516(1) –**<br><br>**Authority limiting type of authorized officials empowered to seek wiretap.** | **18 USC § 2518(4)(d) –**<br><br>**Authority requiring identity of authorizing official be reflected in the order permitting wiretaps.** |
| (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 –<br>. . . .<br><br>(iii) the interception was not made in conformity with the order of authorization or approval. | 1) The Attorney General, Deputy Attorney General, Associate Attorney General, or any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General or acting Deputy Assistant Attorney General in the Criminal Division specially designated by the Attorney General, may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant in conformity with section 2518 of this chapter an order authorizing or approving the interception of wire or oral communications by the Federal Bureau of Investigation, or a Federal agency having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of – [various enumerated offenses]. | (4) Each order authorizing or approving the interception of any wire, oral, or electronic communication under this chapter shall specify –<br><br>(d) the identity of the agency authorized to intercept the communications, and of the person authorizing the application; |

The Title III provisions regarding authorizing officials can be roughly summarized as follows:

- **Section 2518(10)(a)(iii):** Authorizes defense challenges to wiretap orders;
- **Section 2518(4)(d):** Requires orders to reflect the identity of the authorizing official;
- **Section 2516(1):** Limits the pool of DOJ officials empowered to authorize an application.

Although these statutory requirements are plain, the government fumbles this essential step with astounding frequency. *See, e.g., Giordano*, 416 U.S. 505, 525-26 (upholding suppression when wiretap application was not approved by designated official, but by Attorney General's Executive Assistant); *United States v. Chavez*, 416 U.S. 562 (1974) (suppressing wiretap proceeds when application had not been approved by Attorney General or designated Assistant Attorney General); *United States v. Traitz*, 871 F.3d 368, 379-80 (3rd Cir. 1989) (upholding wiretaps when contested application and order identified the authorizing official by title, but not by name); *United States v. Camp*, 723 F.2d 741, 744 (9th Cir. 1984) (permitting the Attorney General to designate the Assistant Attorney General by job title rather than name); *United States v. Citro*, 938 F.2d 1431, 1435 (1st Cir. 1991) (permitting the Attorney General to designate Assistant A.G.'s by title, rather than by name).

Not all courts are bothered by sloppy government compliance with these wiretap requirements. In *United States v. Callum*, 410 F.3d 571 (9th Cir. 2005), for example, the Ninth Circuit held that suppression was not required where a wiretap application failed to identify any official who authorized the application. *Id.* at 576. The very next year, however, the same court ruled that wiretap proceeds should have been suppressed where the wiretap application incorporated the wrong authorization letter. *See United States v. Staffeldt*, 451 F.3d 578, 579 (9th Cir. 2006). Given the difficulty of predicting whether a particular facial violation will result in suppression of the wire, no such violations should be overlooked.

### B. *Sealing Requirements*

Because of privacy concerns, Title III has strict sealing requirements for information intercepted during a wiretap. The statute requires that "[i]mmediately upon the expiration of the period of the order [authorizing wiretapping], or extensions thereof, such recordings shall be made available to the judge issuing such order *and sealed under his directions*." 18 USC § 2518(8)(a) (emphasis added). As the Ninth Circuit has explained, "The government must follow these procedures or it cannot use the intercepted communications against the surveilled individual in a criminal trial. To use wiretap evidence, the government must (1) seal the tapes immediately or (2) provide a 'satisfactory explanation' for the delay in obtaining a seal." *United States v. McGuire*, 307 F.3d 1192, 1202-03 (9th Cir. 2002) (citing *United States v. Pedroni*, 958

F.2d 262, 265 (9th Cir.1992)).

Accordingly, an early task in wiretap litigation is to visit the facility where the original tapes or data was stored and examine the sealing orders and logs for the data.

As with the "authorizing official" challenge, courts often find ways to avoid the strict sealing requirements of Title III. *See, e.g.*, *McGuire*, 307 F.3d at 1203-04 & n. 12 ("We need not decide, however, whether a court order directing that final sealing shall occur in the future amounts to a 'sealing' under the statute. Assuming that the delays in this case were three, twelve, one-hundred twenty-four, and one-hundred twenty-seven days, we hold that the government has provided a 'satisfactory explanation' for the delay in obtaining a seal."); *United States v. Reed*, 575 F.3d 900, 914 (9th Cir. 2009) (holding that sealing delay did not require suppression because it was attributable to court's full calendar, and rejecting argument that failure to seal call data, as opposed to call content, violated § 2518(8)).

### C. *Minimization Challenges*

Title III requires that wiretaps be monitored so as to minimize interception of calls that are irrelevant or fall outside the scope of the wiretap authorization:

> 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.

18 USC § 2518(5). "This minimization requirement spotlights the interest in confining intrusions as narrowly as possible so as not to trench impermissibly upon the personal lives and privacy of wiretap targets and those who, often innocently, come into contact with such suspects." *United States v. Hoffman*, 832 F.2d 1299, 1307 (1st Cir. 1987); *see also United States v. Capra*, 501 F.2d 267, 276 (2d Cir. 1974) (suppressing evidence obtained from calls to a known non-conspirator).

In analyzing the government's minimization efforts, courts typically look to several factors: "1) the nature and complexity of the suspected crimes; 2) the thoroughness of the

government's precautions to bring about minimization; and 3) the degree of judicial supervision over the surveillance process." *United States v. Lopez*, 300 F.3d 46, 57-58 (1st Cir. 2002).

In reality, minimization challenges are often labor-intensive, and low-return, attacks. *See, e.g., United States v. Bennett*, 219 F.3d 1117, 1124 (9th Cir. 2000) (minimization requirement met where improperly intercepted calls accounted for only 3.65% of 7322 total intercepted calls); *Lopez*, 300 F.3d at 57-58 (rejecting minimization attack given small number of non-minimized calls, and lack of prejudice relating to these calls). Where the government has implemented passable training and monitoring procedures, courts are reluctant to second-guess agents' judgments that a call was pertinent to the investigation. *See United States v. Rivera*, 527 F.3d 891, 906 (9th Cir. 2009) (noting that the determination whether a call should be labeled pertinent "is inevitably a judgment call," and finding minimization efforts sufficient where 203 of 4,651 calls were minimized); *McGuire*, 307 F.3d at 1201 (holding that "[l]aw enforcement is entitled to latitude to scrutinize messages by conspirators, because such messages may contain double-meaning and implied purposes, or even be conveyed in secret code"). Unless you can point to specific calls that should have been minimized but were not, a minimization challenge may not be a fruitful line of attack.

### D. *Territorial Jurisdiction*

Just argued before the Supreme Court is *United States v. Dahda*, No. 17-43 where the Court heard arguments on whether a wiretap must be suppressed where it was obtained pursuant to a wiretap order that is facially insufficient because the order exceeds the judge's territorial jurisdiction. The Kansas district court order authorized surveillance of certain cellphones even if they were transported outside of the judicial district. The parties agreed that the order violated Title III's general requirement that district courts authorize intercepts only within their own territorial jurisdiction in violation of 18 U.S.C. § 2518(3). Evidence may be suppressed if derived from a wiretap order that is "insufficient on its face." 18 U.S.C. § 2518(10)(a).

## IV. "NECESSITY" SHORTCOMINGS AS A CHALLENGE TO ELECTRONIC INTERCEPTIONS

### A. *Necessity and Normal Investigative Techniques*

The first of the "substantive" defense attacks for wiretaps is the *necessity* requirement.

Because wiretaps are so extraordinarily invasive, Congress intended the procedure to be used only when traditional investigative methods have been tried and failed. *See Giordano*, 416 U.S. at 515 ("These procedures were not to be routinely employed as the initial step in criminal investigation. Rather, the applicant must state and the court must find that normal investigative procedures have been tried and failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous.").

Title III requires that a wiretap application include "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." 18 USC § 2518(1)(c). Similarly, a wiretap order must reflect a determination that the procedure is necessary: "Upon such application the judge may enter an ex parte order . . . authorizing . . . interception of . . . electronic communications . . . if the judge determines on the basis of the facts submitted by the applicant that . . . . normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous." 18 USC § 2518(3)(c)(3). "These two sections together make up the so-called necessity requirement for granting a wiretap order. The statutory language suggests that before finding that a wiretap is necessary, the court must find that alternative methods have been tried or would not have succeeded." *United States v. Ippolito*, 774 F.2d 1482, 1485 (9th Cir. 1985). Electronic interceptions should not be permitted if "traditional investigative techniques would suffice to expose the crime." *United States v. Kahn*, 415 U.S. 143, 153 & n.12 (1974).

What normal investigative techniques must be exhausted before the government resorts to a wiretap? Here is a list to explore when examining the sufficiency of the government's investigative efforts before a wire:

- Search warrants
- Grand jury testimony/subpoena
- Infiltration by undercover agents
- Surveillance
- Trash covers
- Financial investigations
- Toll registers (phone records)
- Witness interviews
- Cooperating witnesses/informants
- Controlled buys
- Video surveillance
- Mail covers
- Pen registers
- Trap and trace

*See generally* S. REP. 90-1097,1968 U.S.C.C.A.N. 2112, 2190 ("The judgment would involve a consideration of all the facts and circumstances. Normal investigative procedure would include, for example, standard visual or aural surveillance techniques by law enforcement officers, general questioning or interrogation under an immunity grant, use of regular search warrants, and the infiltration of conspiratorial groups by undercover agents or informants.")

Acts of violence may enter into the necessity calculus. Risk of violence alone, however, cannot justify a wiretap absent a showing that other investigative methods have been tried and failed. Even immediate and known threats of violence do not lessen the statutory requirements of Title III. *See, e.g., United States v. Meling*, 47 F.3d 1546, 1556 & n.2 (9th Cir. 1995) (FBI's urgent interest in preventing further poisonings was not justification for deliberate or reckless misrepresentations in wiretap applications).

In *United States v. Rajaratnam,* 719 F.3d 139, 156 (2d Cir. 2013), the affidavit did not disclose "that the SEC had for several years been conducting an extensive investigation into the very same activity the wiretap was intended to expose[,] using many of the same techniques the affidavit casually affirmed had been or were unlikely to be successful." Despite the enormity of the failure to disclose these material facts and their results, the second circuit upheld the use of the wiretaps finding that the failure to disclose was not reckless and not material turning Title III upside down.

### B. *Specificity and Boilerplate*

The government's greatest tool for wiretaps is a computer and word-processing software, with which an agent can copy and paste boilerplate language from previous applications. Particularly of late, Circuit courts have rejected the government's increasing use of boilerplate language in support of its necessity showing. As the Ninth Circuit has explained, the government cannot simply rest on generalizations, but instead "must allege *specific circumstances* that render normal investigative techniques particularly ineffective or the application must be denied . . . . The reason for requiring specificity is to prevent the government from making general allegations about classes of cases and thereby sidestepping the requirement that there be necessity in the particular investigation in which the wiretap is sought. *Ippolito*, 774 F.2d at 1486 (emphasis added) (internal citations omitted).

While the government, in satisfying the necessity requirement, need not exhaust all alternative means of investigation, "neither should it be able to ignore avenues of investigation that appear both fruitful and cost-effective." *Id.* As the Court in *Ippolito* observed, "We would flaunt the statutory intent that wiretaps be used only if necessary, were we to sanction a wiretap simply because the government pursued some 'normal' investigative strategies that were unproductive, when more fruitful investigative methods were available." *Id.*

The government cannot skirt the necessity requirement by simply stating the investigating agent's conclusion that traditional investigative techniques will not suffice to expose the crime. Requisite necessity cannot be shown by "bare conclusory statements that normal techniques would be unproductive." *United States v. Ashley*, 876 F.2d 1069, 1072 (1st Cir. 1989). The affiant cannot rely on "mere boilerplate recitations of the difficulties of gathering usable evidence," in place of specific factual allegations explaining why a normal investigation will not succeed. *United States v. Kerrigan*, 514 F.2d 35, 38 (9th Cir. 1975); *see also United States v. Rivera*, 527 F.3d 891, 899 (9th Cir. 2009) (requiring that wiretap affidavit "[do] more than recite the inherent limitations" of using particular investigative techniques and instead explain "in reasonable detail" why each technique is unlikely to succeed).

One of the best cases on "necessity boilerplate" is the Ninth Circuit's decision in *United States v. Blackmon*, 273 F.3d 1204 (9th Cir. 2001). In *Blackmon*, the FBI obtained wiretap authorization to investigate a suspected narcotics trafficker named Maurice Miller. *Id.* at 1206. Within six months of the authorization of the Miller wiretap, three additional wiretaps (which the government called "spin-offs" of the initial Miller wiretap) were authorized. *Id.* These three subsequent wiretaps involved telephones primarily used by the appellant-defendant Rodney Blackmon. *Id.*

The necessity section of the FBI application for the Blackmon wiretap was, with a few alterations, a duplicate of the Miller wiretap application. *Id.* The Blackmon wiretap produced substantial evidence implicating Blackmon in drug trafficking activity. *Id.*

The Ninth Circuit held that the Blackmon wiretap application did not meet the Title III necessity requirement for two "interrelated" reasons. *Id.* at 1208. First, the application, which was nearly a carbon copy of a previous application for a different suspect, contained material

misstatements and omissions regarding the necessity for the wiretap. *Id.* Second, purged of the material misstatements and omissions, the application contained only generalized statements that would be true of any narcotics investigation. *Id.* Important to the court's analysis was the fact that the *Blackmon* wiretap affidavit contained "boilerplate assertions" that were "unsupported by specific facts relevant to the particular circumstances of this case" and that "would be true of most if not all narcotics investigations." *Id.* at 1210-11 (citing *United States v. Kalustian*, 529 F.2d 585, 588-89 (9th Cir. 1976)). Lest the requirements of section 2518 be rendered "nullities," the court held that "[t]he government may not cast its investigative net so far and so wide as to manufacture necessity in all circumstances." *Id.* at 1211.

Note, however, that courts are deferential to claims of necessity in large conspiracy cases, where the government can—and does—routinely assert that traditional investigative techniques will not suffice to discover the full scope of the scheme. *See Rivera*, 527 F.3d at 900 ("[W]hile physical surveillance in combination with the use of confidential source may have provided the government with enough evidence to arrest and prosecute a few members of the Rivera organization for drug crimes, it is clear from the affidavit that the government required additional evidence to accomplish its purpose of uprooting the entire drug trafficking conspiracy."); *United States v. Forrester*, __ F.3d __, 2010 WL 2977722, at *11 (finding necessity despite successes of traditional techniques because such techniques "could not establish the identities of all conspirators or provide evidence of the purpose and content of conspiratorial meetings"). Unfortunately, this exception too often swallows the rule. *See Rivera*, 527 F.3d at 903-04 ("While the government could probably have relied on [traditional] techniques alone to successfully prosecute a few individuals . . . for drug crimes, the issuing court did not abuse its discretion in concluding that the wiretap was necessary to identify the full scope of the Rivera organization and 'develop an effective case' against its members.") (citation omitted); *United States v. Canales-Gomez*, 358 F.3d 1221, 1225 (9th Cir. 2004) ("The affidavit adequately explained that the interception of wire communications was the *only* way to identify and investigate the whole of the network, including the entire hierarchy of suppliers, transporters, distributors, customers, and money launderers."). The only option for industrious defense counsel is to hold the government's feet to the fire by demanding an accounting of

everything the government cannot reasonably achieve through traditional techniques, while reminding the court that a *de facto* conspiracy exception to the necessity requirement defeats the requirement altogether.

### C. *No Bootstrapping From Previous Investigations or Applications*

The government often attempts to bootstrap necessity showings from previous investigations into subsequent applications for lines or re-ups. That approach has been rejected by the appellate courts. *See, e.g., United States v. Santora*, 600 F.2d 1317, 1321-22 (9th Cir.), *as amended,* 609 F.2d 433 (9th Cir. 1979) (emphasizing that necessity must be shown as to *each* wiretap affidavit and application, and suppressing subsequent wiretaps because reliance on an initial affidavit "was not sufficient to establish that alternative investigative techniques would not succeed with respect to other suspected conspirators whose telephones were later tapped").

This principle is illustrated by the Ninth Circuit's *Gonzalez* decision. *United States v. Gonzalez*, 412 F.3d 1102 (9th Cir. 2005). In *Gonzalez*, the government investigated a large-scale smuggling operation out of Arizona. The investigation was quite successful, with agents infiltrating the bus company involved and securing wiretaps on an Arizona bus facility. The government continued, however, to seek wiretaps on an office in Los Angeles, owned by executives associated with the bus company under investigation. The wiretap applications were granted, and that facility was tapped.

The Los Angeles wiretaps were challenged by the corporation charged and by ten individual defendants. The district court granted a *Franks* evidentiary hearing and ultimately suppressed the proceeds of these wiretaps based on the government's failure to show Title III necessity. On appeal, the Ninth Circuit undertook a detailed analysis of the necessity shortcomings as to the Los Angeles wiretap. It concluded that "the government side-stepped its responsibility to use promising traditional techniques when it began to investigate the Blake Avenue office, and instead conducted only the most cursory investigation before seeking a wiretap." *Id.* at 1113-14. Specifically, the court rejected the government's attempt to import its necessity showing from the earlier Arizona investigation:

> To cover its failure to establish necessity for the Blake Avenue wiretap, the Hill affidavit attempted to shoehorn the significant investigatory work the government conducted before applying for the Terminal wiretap into its application for the Blake Avenue wiretap. *But the government is not free to transfer a statutory showing of necessity from one application to another – even within the same investigation. This court has held that an issuing judge may not examine various wiretap applications together when deciding whether a new application meets the statutory wiretap requirement. Each wiretap application must separately satisfy the necessity requirement.*

*Id.* at 1115 (emphasis added).

Accordingly, the necessity rule is that each wiretap application must stand on its own. *Gonzalez* prohibits importing necessity from a previous investigation to justify a wiretap on a subsequent investigation. Similarly, the government cannot aggregate necessity from other wiretap applications to collectively show necessity for a subsequent application. *See United States v. Carneiro*, 861 F.2d 1171, 1176 (9th Cir. 1988) (holding that district court erred by failing to consider whether each separate wiretap application established necessity on its own). *But see United States v. Garcia-Villalba*, 585 F.3d 1223, 1231-32 (9th Cir. 2009) ("This does not mean, however, that a district court must view a wiretap application in a vacuum. Although the government may not rely on the conclusion that a previous wiretap was necessary to justify the current application, historical facts from previous applications, particularly those within the same investigation, will almost always be relevant.").

The need for individualized necessity and probable cause showings often is at issue in extension applications. Extension applications are not merely a formality that automatically extend an original wiretap. Instead, the "necessity" threshold for an extension application should be higher than that of the original wiretap.

Section 2518(5) of Title 18 requires that each application for an extension of a wiretap must include a full statement of facts regarding necessity, as is required for original applications under section 2518(1)(c). There is, however, an additional statutory requirement in Title III for extension applications. Section 2518(1)(f) specifically requires an extension affidavit to provide "a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results." 18 USC § 2518(f).

The Supreme Court has acknowledged these separate requirements for extension applications. In *Giordano*, the Court observed that "extension orders do not stand on the same footing as original authorizations . . . but are provided for separately." *Giordano*, 416 U.S. at 530. It then emphasized the additional showing required by Section 2518(1)(f). *Id.* The Court found a common-sense rationale for this greater showing:

> Plainly the function of § 2518(1)(f) is to permit the court realistically to appraise the probability that relevant conversations will be overheard in the future. If during the initial period, no communications of the kind that had been anticipated had been overheard, the Act requires an adequate explanation for the failure before the necessary findings can be made as a predicate to an extension order.

*Id.*

Thus, each extension application (or supporting affidavit) must not only explain why the wiretap investigation was necessary in the first instance, but *also* why the earlier wiretaps have not yielded the expected results. *See United States v. Brone*, 792 F.2d 1504, 1506 (9th Cir. 1986); *United States v. Williams*, 737 F.2d 594 (7th Cir. 1984); *United States v. Abascal*, 564 F.2d 821, 826 (9th Cir. 1977).

### D. *The "Good Faith" Requirement for Necessity Showings*

Wiretaps produce huge returns and valuable evidence for the government. Not surprisingly, in many wiretaps the government "manufactures necessity" by conducting only the most cursory investigation before resorting to a Title III application. The defense bar should counter that Title III includes a requirement that traditional investigative procedures be undertaken in good faith.

This "good faith" language can be found in many appellate Title III decisions. *See, e.g.*, *United States v. Spagnuolo*, 549 F.2d 705, 710 (9th Cir. 1977) ("These decisions permit us to make the following observations. To show that 'other investigative procedures have been tried and failed' the affidavit must reveal that normal investigative techniques have been employed *in a good faith effort* to determine the identity of those violating the law and to *assemble sufficient evidence to justify their prosecution* and that these efforts have failed to achieve their ends. The *good faith effort* need not have exhausted all possible uses of ordinary techniques.") (emphases added); *see also United States v. Staves*, 383 F.3d 977, 980 (9th Cir. 2004) ("The issuing judge

must determine whether there is probable cause and if the wiretap is necessary because normal investigative procedures, *employed in good faith*, have failed, would likely be ineffective, or are too dangerous.") (emphasis added). If the pre-wire investigation appears *pro forma*, considering pushing this undeveloped area of Title III law.

## V. PROBABLE CAUSE SHORTCOMINGS IN WIRETAP APPLICATIONS AND ORDERS

### A. *The Three P.C. Requirements of Title III*

A wiretap application (and the resulting order) must establish probable cause in relation to three facts: i) that an individual is committing a crime, ii) that communications about that crime will be intercepted, and iii) that the phone line tapped is being used to communicate about the crime. These three probable cause requirements are codified in Title III:

> (3) Upon such application the judge may enter an ex parte order . . . . 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;
> >
> > . . . .
> >
> > (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.

18 U.S.C. § 2518(3)(a)(b) & (d).

Federal courts have interpreted the probable cause showing required in Title III as the same as the showing required for search warrants under the Fourth Amendment. *See, e.g., United States v. Macklin*, 902 F.2d 1320, 1324 (8th Cir. 1990) ("The probable cause showing required by section 2518 for electronic surveillance does not differ from that required by the fourth amendment for a search warrant."); *see also United States v. Talbert*, 706 F.2d 464, 467 (4th Cir.1983); *United States v. Fury*, 554 F.2d 522, 530 (2d Cir. 1977); *United States v. Falcone*, 505 F.2d 478, 481 (3d Cir.1974). That standard was concisely described by the

Supreme Court in *lllinois v. Gates*:

> The task of the issuing magistrate is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, including the "veracity" and "basis of knowledge" of persons supplying hearsay information, there is a fair probability that contraband or evidence of a crime will be found in a particular place.

*Illinois v. Gates*, 462 U.S. 213, 238 (1983).

Although the probable cause standard for wiretaps is the familiar Fourth Amendment test, the Supreme Court has stressed that Fourth Amendment privacy concerns underlying electronic interceptions make this cause inquiry particularly important:

> The need for particularity and evidence of reliability in the showing required when judicial authorization of a search is sought is especially great in the case of eavesdropping. By its very nature eavesdropping involves an intrusion on privacy that is broad in scope. As was said in *Osborn v. United States*, 385 U.S. 323, 87 S.Ct. 429, 17 L.Ed.2d 394 (1966), the "indiscriminate use of such devices in law enforcement raises grave constitutional questions under the Fourth and Fifth Amendments," and imposes "a heavier responsibility on this Court in its supervision of the fairness of procedures."

*Berger*, 388 U.S. at 56.

### B. *Is the Individual Committing a Crime?*

As with a traditional search warrant affidavit, a wiretap application must establish that the target has committed or is committing a crime. 18 USC § 2518(3)(a). There are limits as to *which* crimes are permissible bases for a wiretap (albeit very broad limits). The statute permits wiretaps for crimes enumerated in 18 USC § 2516. That statute, in turn, provides a laundry list of federal offenses ranging from assassination of the President to obscenity. *Id.* The classic wiretapping subjects – drugs, guns, and conspiracies relating to the two – fall squarely within the statute. If the wiretap produces unusual charges, it is worth it to check Section 2516 to make sure the crime is enumerated.

### C. *Will Communications about the Crime be Intercepted?*

Before obtaining a wiretap, the government must show probable cause that communications about the crime will be intercepted. 18 USCA § 2518(3)(b). There are comparatively few cases addressing this aspect of the P.C. showing – in essence, an argument that the targeted device (typically phones) wasn't used to facilitate the crime. The *Giacalone*

case may be the typical resolution for this attack. *United States v. Giacalone*, 853 F.2d 470, 480 (6th Cir. 1988). In *Giacalone*, it was clear that there was probable cause that the defendants were engaged in extortion. The challenge was that there was no probable cause that the defendants *used phones* to extort people – they preferred their extortion face-to-face. *Id.* The Sixth Circuit was unimpressed with this clever argument: "[R]eading the whole affidavit in a common sense manner, Judge Taylor could reasonably have found probable cause to believe that incriminating communications would be intercepted at the Farm Fresh premises, as required by 18 U.S.C. § 2518(3)(b), and that the telephones to be monitored were either being used in connection with the criminal activity or were commonly used by the suspects, as required by 18 U.S.C. § 2518(3)(d)." *Id.*

### D. *Are There Criminal Communications On the Target Line?*

The final probable cause requirement is whether a specific target line (a specific phone number) is being used for criminal conversations. 18 USCA § 2518(3)(d). This is obviously closely related to the second probable cause requirement, that "particular communications" regarding crimes will be intercepted (section 2518(3)(b)). Many cases discuss subsections (3)(b) and (3)(d) in the same analysis.

Beware that subsection (3)(d) is disjunctive – the government can establish probable cause either by showing criminal activity on a target line or by showing the target's association with that line. *United States v. Edwards*, 124 F. Supp. 2d 387, 410 (M.D. La. 2000) ("Notably, § 2518(3)(d) contains a disjunctive requirement for probable cause as it relates to the place to be searched. Section 2518(3)(d) permits the judge to authorize surveillance when there is probable cause to believe that either the place to be searched is being used or is about to be used in the commission of a crime, or if the place is listed in the name of or is commonly used by such person. Thus, even if the Court was not persuaded that Santini's affidavit presented a sufficient connection between Edwin Edwards' alleged schemes and the Jamestown Avenue office, the affidavit established that the Jamestown office was 'commonly used' and 'leased by' Edwin Edwards. The requirements of this section would, therefore, be satisfied.").

### E. *Other Probable Cause Issues*

#### 1. Non-Targets and Probable Cause

Once the government has established probable cause that a target will be discussing crimes on a particular phone, must it also establish that other people likely to be caught on the tap will *also* be involved in criminal conversations? The Ninth Circuit has held that there is no such requirement. *See United States v. Martin*, 599 F.2d 880, 884 (9th Cir. 1979), *overruled on other grounds by United States v. DeBright*, 730 F.2d 1255 (9th Cir. 1984).

In *Martin*, the defendant complained that while the government listed him as a "probable conversant," it failed to establish probable cause that he was engaged in criminal activity. *Id.* at 884. (Notably, he was not the listed target of the investigation.) The Ninth Circuit found no constitutional requirement for such a showing, and further held that it was not required by Title III. *Id*. at 885 ("Section 2518(3)(a) permits a judge to issue an authorization order upon a showing that probable cause exists with respect to an individual; it does not expressly require a similar showing with respect to each person named in the application.")

The *Martin* rule effectively enables the government to sidestep the probable-cause showing as to the real target of the investigation. On the one hand, the government can argue that a wiretap is necessary because traditional investigative techniques will not suffice to develop evidence against a particular target; on the other hand, the government need not show that the same target will be caught on the wire. To date, however, courts of appeal have not been bothered by this tension. For example, in *United States v. Reed*, 575 F.3d 900 (9th Cir. 2009), the Ninth Circuit held that agents did not have to discontinue a wiretap upon discovering that the actual user of a tapped line was different from the user for whom probable cause was shown in the wiretap application. *Id.* at 910. The court reasoned that authorization for a wiretap is based on probable cause to believe that a *phone* is being used; its user need not be identified at all. *A fortiori*, establishing probable cause as to the wrong user is not fatal to a wiretap and does not require suppression. *Id.*

In United States v. Carey, 836 F.3d 1092, 1093 (9th Cir. 2016), federal agents secured a wiretap against their target, Escamilla. At some point, they realized the target wasn't using this line. Based on the use of these calls the defendant, Carey moved to suppress arguing that the tap was used to listen to him when he wasn't involved in the conspiracy under surveillance. The Court adopted a "plain hearing" rule when agents overhear speakers unrelated to the target

conspiracy while listening to a valid wiretap when they haven't complied with probable cause and necessity as to those specific speakers. 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.

**2.** Staleness and Probable Cause

Like affidavits underlying search warrants, affidavits in support of electronic interceptions must be based on information that is sufficiently current to support a finding of probable cause. *See, e.g., United States v. Domme*, 753 F.2d 950, 953 (11th Cir. 1985) ("As with other types of search warrants, the probable cause needed to obtain a wiretap must exist at the time surveillance is authorized . . . . It does not satisfy the probable cause standard if the government can demonstrate only that the items to be seized could have been found at the specified location at some time in the past. Rather, the government must reveal facts that make it likely that the items being sought are in that place when the warrant issues.") (internal citations omitted); *United States v. Tefhe*, 722 F.2d 1114, 1119-20 (3d Cir. 1983) ("The factors affecting staleness are more easily applied in cases of tangible property, rather than wiretaps. However, the rationale is still valid.").

## VI. *FRANKS* CHALLENGES TO ELECTRONIC INTERCEPTIONS

### A. *Franks and Title III Challenges*

The final category of wiretap challenges involves *Franks* issues. In the familiar Fourth Amendment context, a defendant may challenge a search conducted pursuant to a warrant on the grounds that the warrant affidavit, even though facially adequate to support probable cause, contained factual misstatements or omissions that influenced the issuing magistrate. *See Franks v. Delaware*, 438 U.S. 154 (1978). If the reviewing court determines that an affiant has knowingly or recklessly included false information that is material to the determination of probable cause, evidence seized pursuant to that warrant must be suppressed. *See United States v. Dozier*, 844 F.2d 701, 705 (9th Cir. 1988).

This reasoning applies with equal force to wiretap affidavits. *United States v. Ippolito*, 774 F.2d 1482, 1485 (9th Cir. 1985). Indeed, because of the "highly intrusive" nature of wiretaps, affidavits in support of them should be evaluated with the utmost scrutiny. *See United*

*States v. Bennett*, 219 F.3d 1117, 1121 (9th Cir. 2000).

The *Franks* legal analysis in the context of a wiretap motion is similar to the *Franks* approach to a search warrant. One significant difference is the impact of the omissions or misstatements upon the government's application; in a wire motion, a *Franks* error may jeopardize not only probable cause, but also necessity for the wiretap. If a wiretap affidavit fails to describe accurately the successes of traditional investigative techniques, the necessity showing is compromised and suppression—or at least a hearing—may be required. *See, e.g., Ippolito*, 774 F.2d at 1485 ("The necessity showing and finding are therefore material to the issuance of a wiretap order and are subject to *Franks*.").

### B. *Misstatements, Falsehoods, and Omissions*

In addition to outright falsehoods, "deliberate or reckless omissions of fact" may also be fatal to a wiretap affidavit. *See United States v. Stanert*, 762 F.2d 775, 780-81 (9th Cir.), *as amended*, 769 F.2d 1410 (9th Cir. 1985) ("The use of deliberately falsified information is not the only way by which police officers can mislead a magistrate when making a probable cause determination. By reporting less than the total story, an affiant can manipulate the inferences a magistrate will draw. To allow a magistrate to be misled in such a manner could denude the probable cause requirement of all real meaning.")

Improper omissions may include a failure to supply known information that bears on an informant's reliability. *See Illinois v. Gates*, 462 U.S. 213, 230 (1983). The Ninth Circuit has accordingly explicitly disapproved the practice of excluding references to an informant's prior criminal history, holding that such information must be made available to the magistrate making a probable-cause determination. *See United States v. Reeves*, 210 F.3d 1041, 1046 (9th Cir. 2000). While recognizing the importance of protecting the confidentiality of police informants, the Court in *Reeves* held that an informant's criminal history could not be so "sanitized" as to completely obscure its "material essence." *Id.*

*Franks* omissions are not limited to leaving out the details of an informant's cooperation deal, or not revealing a cooperator's prior convictions for crimes of dishonesty. The Ninth Circuit has also held that omitting the successes of traditional investigative methods can constitute *Franks* error, because it impairs the authorizing court's ability to evaluate necessity.

*See United States v. Simpson*, 813 F.2d 1462 (9th Cir. 1987). In *Simpson*, the federal affiant alleged that the conspirators "had insulated themselves and their high-echelon accomplices from all but a small circle of associates," such that "undercover agents, confidential informants, and witnesses could not penetrate the organization to the highest levels because of insulation tactics utilized." *Id*. at 1471. The affiant in *Simpson* did not fully reveal the extent to which the government had infiltrated a drug conspiracy. *Id.* at 1471-72. The Ninth Circuit upheld the district court's suppression of the electronic interceptions. *Id.* As the Court explained, "Here, the specific facts withheld from the issuing judge about this particular investigation reveal that traditional techniques could have led to the successful infiltration of the entire enterprise." *Id.* at 1472-73.

When a defendant makes a preliminary showing that an affidavit (1) "contains intentionally or recklessly false statements or misleading omissions," and (2) "cannot support a finding of probable cause without the allegedly false information," he is entitled to a *Franks* hearing to flush out the nature and extent of the affidavit's deficiencies. *Reeves*, 210 F.3d at 1044. The defense need not *prove* the *Franks* error at this stage – a "substantial showing" will earn an evidentiary hearing. *Gonzalez*, 412 F.3d at 1111 ("Our case law does not require clear proof of deliberate or reckless misrepresentations at the pleading stage . . . . Instead, at this stage we simply require the defense to make a substantial showing that supports a finding of intent or recklessness.")*)* (citation omitted).

### C. *Taint from Previous Wiretaps*

Bear in mind that *Franks* errors in earlier wiretaps (or necessity and probable cause shortcomings) can taint later wiretaps that rely upon those proceeds. If an original wiretap was improvidently granted, the government cannot use the fruits of that wiretap to obtain authorization for later interceptions. *See, e.g., United States v. Giordano*, 416 U.S. 505, 529-30 (1974) ("Even though suppression of the wire communications intercepted under the October 16, 1970, order is required, the Government nevertheless contends that communications intercepted under the November 6 extension order are admissible because they are not

'evidence derived' from the contents of communications intercepted under the October 16 order within the meaning of § § and 2518(10)(a). This position is untenable."); *United States v. Vento*, 533 F.2d 838, 847 (3d Cir. 1976) ("If the government's application did not present probable cause for the authorization of the interception, then the authorization and any surveillance pursuant to it were improper. And, if the surveillance was improper, the government could not use the fruits of that surveillance at trial or to further its investigation."); *United States v. Arreguin*, 277 F. Supp. 2d 1057, 1059 (E.D. Cal. 2003) (holding that evidence obtained through a federal wiretap was necessarily evidence obtained by virtue of an earlier state wiretap upon which the federal wiretap application relied).

## VII. PRACTICAL POINTERS FOR WIRETAP LITIGATION

Following are some general pointers on wiretap litigation.

· **Early Disclosure of Wiretap Applications and Ten-Day Reports**: Title III requires that wiretap applications and orders be disclosed ten days before wiretap proceeds are used in a hearing. *See* 18 USC § 2518(9). Although this was presumably intended for evidentiary hearings and trial, this disclosure provision has also been held to apply to *detention* hearings. *See United States v. Salerno*, 794 F.2d 64 (2d Cir. 1986), *rev'd on other grounds*, 107 S. Ct. 2095 (1987) ("We think it clear that Congress intended § 2518(9) to apply to detention hearings.") Early and aggressive invocation of this right can help back government counsel off of relying on wiretap proceeds in bail hearings (as an AUSA rarely has disclosure ready that early in the case).

· **Early identification of cooperating informants:** Wiretaps are expensive and time-consuming, and are typically only used in fairly serious cases. With the corresponding high federal sentencing exposures, the likelihood that co-defendants will flip and become cooperating witnesses increases.

It is common for a wiretap application to refer to cooperating witnesses or informants by code name – and those informants' identities typically will not be disclosed, because they will not be used at trial. Every co-defendant who cooperates early in the case represents a lost opportunity to identify these wire informants.

One of the earliest tasks in a wiretap should therefore be to cull all references to the

cooperating wire witnesses and informants, and prepare short and easy-to-read memos listing their characteristics. These memos should be distributed to all defendants, and counsel should aggressively push their clients to try to identify the informants. Delay on this chore can mean that the one defendant who knew a cooperating wire informant may be lost to the lure of a § 5K1.1 deal.

· **View the Physical Documents**: It pays to be a skeptic in wiretap litigation. For example, in a recent wiretap in the Northern District of California, the government completely failed to attach a referenced affidavit to a wiretap extension application. The application was nonetheless approved. That dramatic omission would have never been detected if someone hadn't gone through all of the hard copy applications and affidavits in the district court clerk's office.

Very close review of the materials actually on file can reveal missing (and essential) attachments, applications that were authorized by the DOJ official *after* the district court issued the wiretap order,[9] and DOJ authorizations that are missing altogether. It is an essential step in mounting a wiretap challenge.

## Conclusion

With the excesses of the USA PROTECT ACT, average citizens have finally been sensitized to the extraordinarily invasive nature of increasingly prevalent wiretaps. Traditional Title III litigation is exhausting and expensive, and it remains an area of law plagued by disingenuous decisions and blessed with few victories. It is, nonetheless, an arena where aggressive defense litigation serves societal goals far beyond any one client's individualized interests.

–oOo–

[9] *See Callum*, 410 F.3d at 577 & n. 8 ("The basis for defendants' claim is that the issuing judge listed the time he signed the wiretap order as 3:00 p.m., nearly half an hour before the timestamp on the fax that constituted DOJ's written authorization of the application.").